CAHIERS DE LA SÉCURITÉ

n°6

La criminalité numérique

Mafias, pédophilie, fraudes, sectes, rumeurs, jihad, propagande, terrorisme, cyberdéfense, normes...

Également dans ce numéro :

La chaîne hiérarchique du ministère public

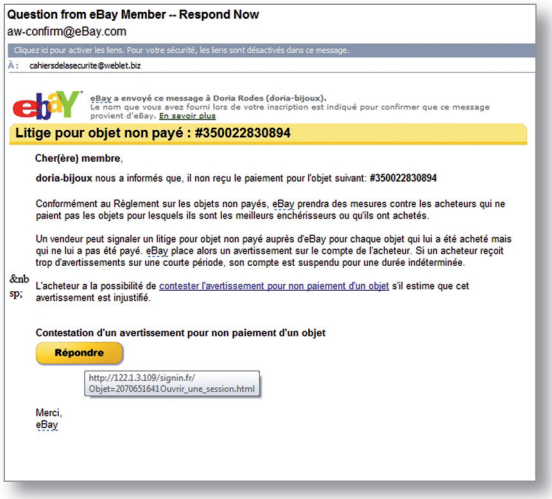
Le compte-rendu des XV^e Journées européennes des représentants de l'État

INHES
INSTITUT NATIONAL DES HAUTES ETUDES DE SÉCURITÉ

octobre-décembre 2008

Le Web et les organisations mafieuses : *mythes et réalités*

Patrice HERNU


Question from eBay Member -- Respond Now
aw-confirm@eBay.com
Cliquez ici pour activer les liens. Pour votre sécurité, les liens sont désactivés dans ce message.
A : cahiersdelasecurite@weblet.biz
eBay a envoyé ce message à Doria Rodes (doria-bijoux).
Le nom que vous avez fourni lors de votre inscription est indiqué pour confirmer que ce message provient d'eBay. En savoir plus
Litige pour objet non payé : #350022830894
Cher(ère) membre,
doria-bijoux nous a informés que, il non reçu le paiement pour l'objet suivant: #350022830894
Conformément au Règlement sur les objets non payés, eBay prendra des mesures contre les acheteurs qui ne paient pas les objets pour lesquels ils sont les meilleurs enchérisseurs ou qu'ils ont achetés.
Un vendeur peut signaler un litige pour objet non payé auprès d'eBay pour chaque objet qui lui a été acheté mais qui ne lui a pas été payé. eBay place alors un avertissement sur le compte de l'acheteur. Si un acheteur reçoit trop d'avertissements sur une courte période, son compte est suspendu pour une durée indéterminée.
  L'acheteur a la possibilité de contester l'avertissement pour non paiement d'un objet s'il estime que cet avertissement est injustifié.
Contestation d'un avertissement pour non paiement d'un objet
Répondre
http://122.1.3.109/signin.fr/Objet=2070651641Ouvrir_une_session.html
Merci,
eBay

Avant que les cybercriminels ne mettent en danger la sécurité de l'État et des entreprises, ceux qui pénétraient les systèmes d'exploitation des premiers ordinateurs étaient simplement des passionnés, supplantés désormais par des réseaux organisés, aux conduites aussi criminelles que celles des mafias. Paradoxalement, alors que les systèmes étaient vulnérables, ils n'étaient attaqués qu'en surface. Maintenant que la sécurité est renforcée, que les lignes de codes se sont sophistiquées, ils sont rendus plus fragiles par l'effet combiné de la complexification et de la vulgarisation des pratiques qui n'échappent donc plus à la criminalité ordinaire et nécessitent une réaction de l'État et de la société.

The Web and the Mafia: Myths and Realities

Before cybercriminals started to exploit the net, the first hackers who threatened state security were those who engaged in the activity for excitement and fame. They have now been replaced by organized crime and mafias. Paradoxically, in the past when systems were most vulnerable, they were only attacked on the surface. Now that their security has been reinforced and defenses are more sophisticated, they have become more fragile under the combined effects of the increased complexity of the instruments used for attacks and their general public diffusion. We have gone beyond the menace of common criminality and entered an era that requires better responses in order protect the state and society.

Patrice Hernu

Économiste de formation, il est diplômé de l'École nationale de la statistique et de l'administration économique (ENSAE). Il est titulaire d'un doctorat d'économie appliquée, d'un doctorat de mathématiques appliquées à la gestion des entreprises et d'un diplôme d'expert fiscal (ENI). Il commence sa carrière à l'Institut national de la statistique et des études économiques (INSEE) en tant qu'administrateur, puis devient sous-directeur du service d'études statistiques et des systèmes d'informations (Sesi) au ministère de la Santé. Depuis 2001, il est conseiller scientifique du ministère de l'Écologie et du Développement durable. Il est également, depuis 2007, conseiller du directeur de l'Inhes.

Snobisme et effet de mode s'étaient conjugués pour inciter à vanter les prouesses de tel ou tel pirate sur la toile : le plus souvent, les mérites de ces nouveaux David du cyberespace sont imaginaires. Le fait est que les supposés Goliath des temps modernes, les grandes entreprises comme les organisations gouvernementales ou non gouvernementales et les bureaucraties dont la culture de sécurité reste le plus souvent obsolète, sont des colosses aux pieds d'argile. Les murailles et les remparts ne tiennent que dans la mesure où la communauté qui les habite se défend de donner les clefs des portes dérobées aux robins des bois, par inadvertance, intérêt, bêtise, perversité ou oisiveté. Tout cela est plus affaire de culture et d'éducation que de hauteur des barricades érigées. Une société libre, comme le prétend être celle du réseau global, ne peut être une société de barrières, de quarantaines et de trousseaux de clefs de protection numérique démultipliés à l'envi.

Oui mais... la criminalité et la délinquance sur l'Internet se développent au rythme de ses interconnexions. Et, les petits génies obscurs en quête d'une célébrité dans la communauté de ceux qui « sont dans le coup de la société moderne » ont laissé la place à de vrais cybercriminels, puis à des organisations de type mafieux, quand leur naïveté généreuse ne les a pas conduits à être totalement instrumentalisés par ces mafias d'un nouveau genre.

Le ministère de l'Intérieur, à l'initiative de la ministre Michèle Alliot-Marie, a intégré le constat, parfois alarmant, de cette évolution et prend les dispositions nécessaires pour tenter, à notre échelle, d'endiguer le phénomène. Évidemment, pour ne pas laisser l'imagination criminelle distancer ceux dont la mission est de nous protéger, tandis que la bataille se joue sur un terrain qui précisément échappe aux contours de l'État traditionnel, il faut se donner les moyens de lutter « à armes égales ». C'est la volonté affichée par la ministre en présentant en février 2008 son plan de lutte contre la cybercriminalité (*cf.* son plan en encadré)

Le temps des pionniers de légende

Quand le temps est venu de raconter l'époque des pionniers, la légende est déjà en marche et le péché originel se mélange tant au plaisir qu'à la grandeur d'âme. Dans une civilisation où l'on cherche à construire en toute chose l'idéal du bien et du mal, ce mélange est de bon aloi. La société de l'Internet n'y échappe pas. Puis, vient le temps où il faut mettre à bas les idées reçues. Le *Far West* n'était pas si grandiose et les hommes pas si différents... Le spam, ce fléau qui consiste à inonder un destinataire de courriels qu'il n'a pas sollicités parce que son adresse a été récupérée par un moyen licite ou illicite, aurait pu fêter ses trente ans en mai dernier. « Spam », ne veut rien dire ou presque [1]! En ce mois de mai 1978, un cadre de la société DEC adresse 400 ou 600 [2] messages sur le réseau Arpanet [3] pour vanter les mérites de nouveaux produits. La réaction fut vive en paroles dès cette première et tout le problème et les risques étaient déjà posés par le major Raymond Czahor, responsable de l'Arpanet. Mais, l'impuissance de l'individu réel face à la société des séries virtuelles apparaît aussitôt. Ce sont les Monthy Python qui comprennent immédiatement le parti pris comique et la réalité de la situation. Ils reprennent, en fait, le sketch de Fernand Raynaud sur la société obsessionnelle de consommation et ses « deux croissants ». Mais, tout s'est inversé et c'est désormais l'offreur qui va créer l'obsession sérielle avant que maintenant, au bout de la chaîne, chacun s'imagine être source. Tandis qu'un couple tente de prendre un petit-déjeuner à la manière de Raynaud, la patronne ne propose en réponse que des plats à base de « spam, spam, spam, spam ». C'est la répétition qui guette la défaillance du gogo, qui guette cet instant où une porte va s'ouvrir et où va s'engouffrer votre ami ou votre ennemi... La mécanique du spam actuel et de tous les zombies qui le servent est née. Elle est encore loin d'être criminelle [4]!

....

(1) En fait, le terme est apparu en 1937 pour désigner du Jambon épicé en boîte (SPiced hAM) et, de ce fait, c'est une marque créée et déposée par Hormel Foods cette année-là ! Ce « pâté » a été largement utilisé par l'intendance des forces armées US pour la nourriture des soldats. Le copyright date de 1944. Il s'agit de la première émergence publique du mot pour désigner un objet repoussant dont on aimerait bien ne pas être le destinataire.

(2) On ne sait déjà plus très bien !

(3) Un réseau professionnel précurseur de l'Internet qui n'aurait dû être utilisé que pour diffuser des informations officielles du gouvernement américain.

(4) Nous n'abordons pas dans cet article certaines activités criminelles exercées via Internet, comme les réseaux pédophiles ou le « squam » (activité apparentée au spam où des émetteurs cherchent à extorquer de l'argent en faisant vibrer les bons sentiments). Dans cette activité, Internet ne sert qu'à accélérer la communication, et les spams ne font que reprendre des techniques vieilles comme le monde auxquelles le courrier postal suffisait auparavant. Nous nous intéressons aux activités criminelles pouvant donner lieu à constitution ou pérennisation d'organisations à orientation mafieuse.

Certes, tout avait déjà été imaginé dans des œuvres de fiction [5] qui ont formaté notre imaginaire et conduit les hackers [6] en herbe à reproduire une forme d'idéal transgressif ou à simuler ces exploits. Les faux exploits jalonnent l'histoire des hackers. Ainsi, le casse virtuel du siècle qu'a failli réussir un jeune russe en 1994. Après avoir fait virer près de onze millions de dollars sur différents comptes à partir de la Citibank, il se révèle incapable de réaliser le mouvement des fonds extorqués ; ses complices sont arrêtés comme lui-même, dans un second temps, à Londres, où il tentait de récupérer une part des fonds. En fait, il avait dû acheter pour 100 $ une « Back Door » du système et avait, comme bien des princes des hackers, voulu s'offrir un peu de gloire éphémère avec l'appât du gain qui n'est rien sans un peu de reconnaissance... La morale est sauve ! Après trois années de prison, bien qu'il ait été un des plus célèbres des génies obscurs, il n'est plus dans la légende vivante. Les vrais surdoués ne l'ont pas fait savoir et sont soit du côté de la vertu affichée – ils dirigent des entreprises de pointe – soit du côté du crime, et l'histoire réelle montre qu'il n'est en réalité pas utile d'être surdoué !

L'histoire véritable de l'industrie du virus est donc une autre histoire. Le premier virus connu, capable d'infecter un ordinateur personnel date de 1982. Destiné à l'Apple II, il se contente d'écrire un poème sur l'écran. Autorépliquant, donc authentiquement viral, il donne des idées, d'abord aux universitaires qui vont immédiatement théoriser le principe et fournir un mode d'emploi à tous les apprentis. En 1986, deux Pakistanais, amateurs sans savoir-faire supérieur à celui de milliers de jeunes informaticiens en herbe, appliquent le manuel et créent le premier virus à succès pour l'IBM PC, « Brain », lequel sera copié, recopié et adapté. Le virus se contentait d'afficher la publicité pour le magasin que tenaient les frères Alvid à Lahore au Pakistan. Mais, faute d'obstacle, le virus fait le tour du monde et provoque une panique. Alors que le monde n'a connu que deux virus principaux, le mythe du cataclysme numérique emporte tout. La presse titre : « Débranchez vos ordinateurs pour éviter la fin du monde ! »

John McAfee imagine alors le profit qu'il peut tirer de cette panique et fait créer [7] le premier antivirus. Dans la foulée, apparaît Norton Antivirus [8]. Cette agitation suscite l'engouement d'autres gamins qui veulent déjouer non pas les machines - jeu d'enfant à cette époque - mais les antivirus ! De plus, ces virus se transmettaient par les disquettes et non par les réseaux, de sorte que leur réputation, celle qui persiste, tout comme les antivirus, a bel et bien précédé la réalité de leur apparition.

Les virus - au sens commun actuel - sont donc en réalité relativement récents. Ils ont été pensés, imaginés et, fait surprenant, combattus avant qu'ils ne se présentent comme des menaces réelles. En 1988, un étudiant en informatique lâche un virus autorépliquant sur l'Internet universitaire. Gros dégâts. Nouveaux progrès des antivirus qui se déportent du secteur d'amorçage des disques [9] vers les fichiers qui exécutent des programmes. Cela donne l'idée, en 1991, à un étudiant de Jérusalem de mettre au point un virus qui dort avec le fichier et le supprime s'il est exécuté un « vendredi 13 » !

Le côté magique de la date n'est pas innocent. Mais, si les antivirus et la menace virale échauffent les esprits dans les universités, spécialement américaines avec un arrière-plan de théorie du complot, le bon peuple tarde à réagir et se contente de fermer le PC les vendredi 13. Assez curieusement, apparaît alors le fameux virus Michelangelo. Oui, Michel-Ange ! Aucun rapport ? Si. Sa date de naissance est en 1992, comme chaque année, le 6 mars. Mais, en 1992, c'est une semaine avant un fameux « vendredi 13 ». Et ce virus est censé effacer les cent premiers secteurs du disque dur et le rendre ainsi inutilisable si le fichier infecté s'exécute le... 6 mars sans être protégé par le fameux antivirus McAfee. Ne tirons aucune conclusion hâtive, mais John McAfee passe en boucle à la télévision pour annoncer que, faute d'antivirus, jusqu'à cinq millions de machine pourraient être infectées. En fait, ni McAfee ni Norton ne purent montrer à la presse le moindre PC infecté par le virus le 6 mars, sauf celui qu'ils avaient infecté eux-mêmes avec une souche dont personne n'eut l'outrecuidance de leur demander où ils l'avaient trouvée.

Bref, nous voilà en 1995, et dès que Windows tombe en panne, « c'est la faute au virus ». Il faut comprendre

••••

(5) Le principe du virus informatique serait apparu dans un roman de John Brunner, *Sur l'onde de Choc* (1975). Il évoque les mécanismes grâce auxquels des programmes seraient capables de passer d'un ordinateur à l'autre sans repérage possible. En fait, il a généralisé le principe d'un premier « ver », le « ver Creeper », capable de se répandre sur un réseau, apparu en 1971.

(6) « Hacker » signifie en anglais *bricoleur*, *bidouilleur* ; il désigne aujourd'hui le détenteur d'une maîtrise technique et vaguement magique lui permettant de détourner ou de contourner un processus numérique pour accéder à des informations ou pour les modifier. Comme la programmation sur Internet se fait par couches successives (couches métiers, couches soft, couches langages, couches d'interface avec le hardware, etc.), il y a donc autant de type et de niveau de « Hacker » qu'il y a de niveaux de programmation et d'objet informatique.

(7) Par Dave Chambers, un jeune de 19 ans, passionné certes...

(8) Écrit par le même Dave Chambers débauché par Peter Norton.

(9) Dit secteur de « boot ». « Donner un coup de pied » pour faire démarrer.

que le virus n'a d'intérêt que s'il sert une activité mafieuse, criminelle ou commerciale - situations très différentes - et que, tant que cet intérêt n'est pas objectivé, il reste, pour l'essentiel, un mythe, réel, éventuellement destructeur, mais qui n'a pas les caractéristiques cataclysmiques qui lui sont prêtées. Or, ces premiers virus ne servent en réalité à rien qu'à faire du bruit, c'est-à-dire à faire parler d'eux-mêmes ou de leur supposé auteur.

Avec l'apparition du Pentium qui interdit de lui-même l'opérabilité de certains virus, les grands éditeurs veulent se dégager de ce secteur... qui n'a plus très bonne réputation. Les virus, ce serait fini ! Mais, en fait, c'est à cet instant que commence la vraie histoire des virus, celle que la légende avait prédite, mais que ni les éditeurs ni les universitaires en mal de notoriété n'avaient réalisée.

Apparaît, en effet, en Bulgarie, le premier virus capable de générer son propre cryptage, et se présentant avec une signature auto-flexible, donc non repérable par les antivirus antérieurs. Il n'a certes d'autre but que d'assurer la promotion des paroles et citations d'Iron Maiden [10]. Cela allait entraîner une nouvelle mutation de ce secteur, d'autant que d'après l'aveu même de David Perry [11], avec la version d'essai de Windows 95, Microsoft avait livré elle-même aux éditeurs d'antivirus le premier virus de macro au monde [12]. De fait, de 1995 à 1999, les entreprises sont visées par ces virus de macro, notamment par ceux qui vont arriver via le réseau et le truchement d'Outlook.

De 1995 à 1999, c'est la naissance et la mort des virus traditionnels. Les hackers n'étaient que de gentils garçons. Ceux qui ont écrit ces virus continuent de travailler, les plus doués pour de grandes maisons. Les hackers se réunissent en congrès et sont passés - pas toujours - du bon côté de la force. Les autres, ceux de la « dark side » se sont mis au service d'organisations mafieuses menées par des criminels. Car, faire un virus n'est plus un art. C'est devenu une industrie. Une question de patience. C'est à la portée de tout informaticien. Un virus a son prix proportionné non pas aux dégâts qu'il peut engendrer, mais aux bénéfices qu'il peut générer pour ceux qui les utilisent. La première attaque Web massive n'a eu lieu que l'année dernière par l'intermédiaire d'un malware acheté à la mafia russe.

Dans notre histoire, nous avions la réalité, les grandes épopées antiques puis la légende, le mythe. En matière de virus, nous avons eu la légende, le mythe, nous entrons maintenant, et maintenant seulement, dans la réalité. Elle nous vient du monde virtuel. Pénétrons sa réalité, celle de la cybercriminalité.

La cybercriminalité, une réalité à combattre

Les bidouilleurs voulaient s'amuser, se faire une publicité à bon compte. Quelques-uns, plus pervers, voulaient détruire votre disque dur, vos données... Mais, c'était l'exception, sauf si ce type de virus était intentionnellement envoyé dans le cadre d'une attaque personnelle. Faites le compte : détruire des données ne fait que la fortune des éditeurs d'antivirus. À moins qu'il ne faille faire mal quelque part pour que chacun songe à se protéger de menaces qui ne nous concerneraient que modérément sinon : le pillage de nos données et non leur destruction, la surveillance de nos relations, la collecte des adresses de nos amis, etc.

Bref, tout comme la biodiversité et le processus de sélection naturelle conduisent à élaborer une société où la lutte aboutit à instaurer des processus d'équilibre, la diversité des virus - il pourrait en naître des milliers chaque jour - conduit à un processus de sélection où le problème n'est plus de les produire, mais de les mettre en état de servir des finalités.

Pour ce qui concerne les finalités criminelles, il faut donc distinguer le cyber-terrorisme dont le but peut être de détruire ponctuellement et la cybercriminalité avide des profits réalisables par le commerce illicite ou l'extorsion d'identité. Mais l'une et l'autre, dans cette nouvelle ère qui a commencé il y a environ deux ou trois ans, ont tout intérêt à ce que l'Internet, « ça marche ». Les criminels n'ont pas intérêt à détruire ni importuner, mais plutôt à « endormir », ce qui explique la fabuleuse et extrême sophistication de l'activité frauduleuse sur l'Internet depuis les années 2000. Qui aurait intérêt à faire tomber en panne nos micros ? Même une attaque terroriste d'État ou non

....

(10) Iron Maiden est un groupe formé en 1975 au Royaume-Uni par le bassiste Steve Harris et son ami d'enfance Dave Murray. Ils furent les pionniers de ce qui fut appelé la NWOBHM (*New Wave Of British Heavy Metal*). Dans une filiation à message du style Punk, il évolue dans une mythologie baroque et virtuelle qui va de la Bible aux grandes figures de l'histoire.

(11) David Perry était un salarié de Norton dans les années 1990. Il est aujourd'hui directeur global pour l'éducation chez l'éditeur d'antivirus Trend Micro. Certains éléments de cet article sont attestés par une interview qu'il a accordée à SVM (*Sciences & Vie Magazine*) sur l'histoire de la sécurité informatique.

(12) « Word Concept Macrovirus », en clair le mode d'emploi pour fabriquer un virus s'infiltrant par le logiciel Word. Écrit par un « salarié inconnu », un bon soldat à moins que ce ne soit par le patron lui-même, il affichait sans détruire : « Cela prouve que je suis ce que je dis ». Il ne restait plus aux éditeurs qu'à attendre pour dire à leur tour : « Je panse, donc je suis » !

gouvernementale a intérêt à se tapir, à se préparer, puis à frapper d'un coup comme pour le 11 septembre. C'est le regain de confiance qui constitue une menace tandis que les risques, en fait, se multiplient.

Les escrocs opèrent sur un champ qui, apparemment, semble échapper au contrôle des États traditionnels. La Chine vient de nous montrer qu'en fait les moyens de contrôle existent et sont même négociables avec les grands pourvoyeurs (officiels) de contenu. Il demeure que la grande majorité des affaires traitées par les services *ad hoc* [13] présentent des ramifications extérieures au territoire national. Les instigateurs se retranchent derrière la multiplication des relais intermédiaires et l'évidente mauvaise volonté de certains États à engager une coopération judiciaire efficace.

La cybercriminalité professionnelle a « malheureusement » étouffé la production traditionnelle des programmes malicieux. Certaines équipes se sont spécialisées dans la production des outils. D'autres assemblent ces outils pour les mettre au service d'autres équipes qui les achètent et les confient enfin aux cyber-hommes de main, lesquels vont gérer l'infrastructure mafieuse mise en place. Architectes, techniciens, ingénieurs, donneurs d'ordre, parrains et complices mafieux constituent un réseau global où chacun ignore l'autre maillon, comme dans les organisations mafieuses traditionnelles, mais ici, sans que cela ne résulte forcément d'une volonté organisatrice, mais de la seule inertie organisationnelle de l'internet. D'où le danger et la démultiplication du modèle depuis que la volonté criminelle fait corps avec l'organisation du réseau.

Une cellule produit le virus, une autre l'armera comme cheval de Troie capable de pénétrer un système local, une autre encore concevra l'architecture du système en assignant des tâches différenciées à ces Troyens. Prenons le cas du « phishing » [14] au stade industriel (Russie, Chine, Inde). Il nécessite certes des intrusions parfois violentes dans certaines machines locales pour les transformer en « zombies » intégrés dans un réseau afin de les utiliser pour relayer les envois de spams et l'hameçonnage final qui caractérise le phishing [15]. Cela permet d'étendre de manière virale la surface du réseau, de masquer les vrais opérateurs et de l'utiliser comme moyen de transmission. Mais, l'intérêt des opérateurs est de se faire aussi discret que possible pour pouvoir utiliser votre machine efficacement. De la même façon, quand le réseau passe à l'attaque en envoyant des liens comportant des hameçons, l'efficacité commande que les machines attaquées fonctionnent aussi bien que possible.

Aussi bien, n'est-il pas curieux que les virus destructeurs aient disparu au rythme auquel les vrais réseaux mafieux se sont eux-mêmes développés ? Question éminemment gênante. Elle explique que la France, notamment, ait décidé de se doter d'une véritable politique offensive en la matière (*cf.* encadré), car un corps qui ne sait plus, par le mal qu'il ressent, qu'il est attaqué, est d'autant plus vulnérable. Un Internet de ouate est évidemment un Internet de tous les dangers surtout avec la démocratisation et le manque d'éducation des usagers sur la forme des menaces.

À l'origine, c'est le virus « Storm Worm » diffusé par voie d'e-mail qui a investi jusqu'à quelques millions [16] de systèmes informatiques. Le Storm botnet a été identifié vers Janvier 2007 [17]. Le Storm botnet a été utilisé dans diverses activités criminelles. Ses contrôleurs, et les créateurs du Storm Worm, n'ont pas encore été identifiés [18].

••••

(13) Police et gendarmerie.

(14) Le phishing recouvre l'ensemble des techniques qui consiste à se faire passer pour un tiers de confiance (site, message, etc.) de manière à obtenir de vous des informations qu'il est possible de rentabiliser financièrement (vol de coordonnées bancaires par exemple). Voir plus loin.

(15) Votre micro-ordinateur est-il intégré sans que vous le sachiez dans un réseau, un « BotNet », de machines zombies ? Un outil gratuit à ce jour vous permet assez aisément de le vérifier : RUBooted. Vous pouvez le télécharger sur www.trendsecure.com. Sans danger ! Ce programme, après détection, est capable d'éliminer la plupart des logiciels malveillants (actuels) qui tournent sur votre machine pour le compte d'un réseau tiers. À l'origine, un botnet est un ensemble de robots IRC qui sont reliés entre eux.

(16) Les estimations varient de 1 à 50 millions de machines. Certains réseaux de la mafia russe auraient cumulé jusqu'à plus de 300 000 machines sous un seul contrôleur global.

(17) Le Storm worm représentait alors 8 % des logiciels malveillants sur les ordinateurs Microsoft Windows. Il ne constitue qu'une des menaces très actives en 2007.

(18) Comme bien des virus actuels, le virus Storm semble malgré tout d'origine russe. Il a sans doute été imaginé par la cybermafia considérée encore récemment comme la plus importante : le RBN ou « Russian Business Network » (petite réserve, car tous les spams viraux que j'ai personnellement reçus depuis un trimestre proviennent d'Inde et, particulièrement, d'un centre qu'il est aisé d'identifier sur *GoogleEarth*. Mais ils utilisent des outils d'origine russe). Le RBN a créé une suite logicielle, le MPack vendu à 1 000 $ aux impétrants qui veulent vendre leurs services aux criminels. Inutile de préciser que ces outils mettent leurs utilisateurs eux-mêmes sous un double contrôle. Ils sont en perpétuelle évolution. Un des derniers venus assure, par exemple, le cryptage de votre disque dur avec une clef inviolable de 1 024 bits. Pour récupérer les données, il faut payer, très cher, la clef et le logiciel de décryptage qui l'accompagne.

Ce virus a été particulièrement étudié. De manière plus inquiétante, il a fait preuve de comportements défensifs [19]. Le botnet a surtout attaqué des cibles spécifiques et notamment certains chercheurs qui tentaient de l'enrayer. Les opérateurs du botnet central ont de ce fait commencé à décentraliser leurs opérations, pour se protéger. Mais, du coup, les spécialistes pensent qu'ils ont vendu des portions du Storm botnet à d'autres opérateurs, et, notamment, à des réseaux mafieux chinois et/ou indiens. Le Storm botnet, traqué désormais par les antivirus nouvelle formule, est, sous cette forme, certes en déclin, mais plusieurs experts en sécurité considèrent que le botnet, dans son principe constitutif, demeure une menace majeure. Pour le FBI (États-Unis), le botnet est un risque majeur d'augmentation des fraudes bancaires, d'usurpation d'identité et de toute une kyrielle d'autres cybercrimes.

Des spécialistes font un autre calcul. À supposer que quatre millions de connexions ADSL standard puissent être instrumentalisées simultanément pour mener une attaque contre la sécurité globale d'un pays, cela représente un volume de bandes passantes plutôt inquiétant. De telles ressources, réparties autour du monde avec une présence significative dans de nombreux pays, signifient que ces réseaux pourraient mener des attaques réparties contre des hébergeurs internet ciblés et, partant, paralyser les données critiques d'un pays pendant un laps de temps suffisant pour distraire l'attention des pouvoirs publics, et laisser mener par d'autres des attaques d'un nouveau genre. Ainsi, seraient réunies les caractéristiques usuelles de la convergence entre terrorisme, mafia et luttes politico-ethno-environnementales qui se retrouvent dans la plupart des conflits extra-étatiques modernes. Ce danger ne peut être ignoré et, dans ce domaine comme dans d'autres, il apparaît que la notion même de sécurité globale appelle une convergence en miroir entre le souci de la sécurité intérieure qui s'intéresse surtout à la cyber criminalité et celui de la défense qui affronte la menace cyber-terroriste.

Au bout de la chaîne des robots mafieux, le phishing et ses dérivés

Les machines zombies, les virus qui instrumentalisent vos micro-ordinateurs pour pirater les adresses de vos connaissances, vérifier si vous avez des relations avec tel ou tel organisme où l'usurpation de votre identité pourrait être source de profit, dresser votre profil pour mieux vous séduire ensuite, tout cela ne fait que créer une opportunité de revenus, est illégal, mais n'est pas encore constitutif du crime (au sens pénal) perpétré par une organisation mafieuse, même si ces réseaux d'opportunité n'existent aujourd'hui à ce niveau que parce que des organisations mafieuses vont les utiliser. Les contrôleurs de ces réseaux d'opportunité, botnets, fichiers d'adresse comportant des millions d'adresses qualifiées [20] ou générateurs de sites simulés vont vendre tout ou partie des outils et systèmes à des réseaux mafieux.

Il y a dix ans, un employé peu scrupuleux vendait pour « dix fois rien » la clef d'une backdoor d'une grande entreprise, le fichier qualifié de ses clients ou le mot de passe administrateur du site à un hacker prétendu de génie. Les vrais hackings furent rares ! Le plus souvent, une once de délinquance servait de base au hacker dont l'activité était certes elle-même délictueuse. Aujourd'hui, le modèle est industriel, et les outils sont, de ce fait, rarement durablement secrets ! Il y a donc de la concurrence dans l'offre des malwares, et les tarifs d'achat par les réseaux mafieux sont hors de proportion avec les bénéfices qu'ils peuvent en tirer, s'ils les utilisent malicieusement.

Au bout de la chaîne, tout se termine donc par la visite sur un site ou l'envoi d'un e-mail où l'usager va être sollicité pour cliquer sur un lien ou une autorisation d'exécution d'un programme qui va se charger du braquage, du piratage des données quand ce n'est pas l'usager lui-même qui les livrera en pensant de bonne foi se trouver ailleurs que là où il est en fait. Plus besoin de virus tordus qui entrent par une porte dérobée pour exécuter une tâche complexe sur votre machine et renvoyer par le réseau,

....

(19) Sous l'action de ses contrôleurs. Si ces virus s'auto-répliquent, ils ne savent pas encore se défendre. Mais gageons que cela viendra. Il est désormais aisé d'imaginer par quels processus.

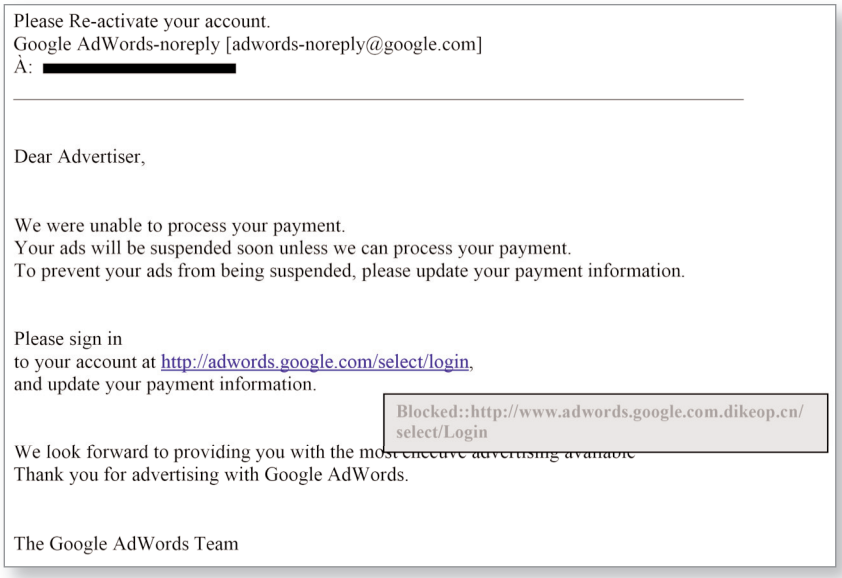
(20) Une adresse n'a vraiment d'intérêt que si elle est qualifiée par rapport à des usages criminels. « Qualifiée » signifie que lui sont attachées des informations pertinentes sur votre profil financier, sexuel, relationnel ou professionnel. Il existe de nombreuses entreprises qui expédient vos e-mails à des milliers de personnes, voire, en France, à deux ou trois millions de destinataires. Elles ont quasiment pignon sur rue et se présentent même comme des agents du respect de la Loi numérique. Envoyer un message publicitaire, légal ou illégal, sur un fichier non qualifié de deux millions d'adresse est à la portée du premier venu. La plupart de ce qu'il faut bien qualifier de spams (le spam commence dès qu'il y a usage d'un robot et ne se limite pas à un seul envoi à une adresse donnée) vont dans la boîte à courrier indésirable. Les programmes mis à disposition par les éditeurs (Microsoft pour Outlook, Thunderbird ou les outils de Firefox) sont relativement efficaces. Mais les grands fauves savent les contourner et leur harcèlement finit parfois par tromper les internautes.

dans votre dos, les informations au commanditaire du fric-frac. C'est l'internaute qui donne l'autorisation et qui ouvre la porte aux cambrioleurs.

La technique est apparemment simple au point que de plus en plus d'amateurs s'y frottent. Ils trouveront sans peine sur Internet un kit [21] leur permettant de jouer aux apprentis mafieux [22]. Quel intérêt pour les laboratoires qui distribuent à prix modique ces générateurs de spam-phishing ? D'abord, cela finance leurs innovations. Ensuite, cela sert de banc d'essai. Enfin, et surtout, cela jette le trouble sur la toile et renforce l'efficacité des vrais « spam-phishers ». En effet, les spams amateurs sont souvent imparfaits. Ils émanent d'une multitude d'individus isolés ne disposant que de quelques adresses IP d'émission, voire d'une seule, aisément repérables et que les salles de veille se préoccupent de suivre pour les fermer. Ces individus opèrent sur des serveurs mutualisés ; il est souvent impossible de fermer totalement ces derniers même si l'exploitant a fait preuve d'une trop grande tolérance. Le fameux « blacklistage » est parfois relativement inefficace, bien que nécessaire, et ne gêne le plus souvent que des contrevenants involontaires. Les vrais mafieux mettent au point des techniques beaucoup plus sophistiquées aptes à tromper réellement. La prolifération de phishings de basse qualité, aisément reconnaissables, contribue à faire passer les meilleurs. D'autant que la multiplication des barrières antivirus, anti-spam, anti-chevaux de Troie, anti-Botnet, anti-toute menace [23], conduit l'usager soit à déléguer à la machine le soin d'autoriser ou de refuser l'exécution des programmes importés (activeX et autres exécutables), soit à cliquer soi-même en série [24], et donc, à autoriser tel lien ou programme proposé par un hameçon qui aura les meilleures apparences... À ce stade, cela relève rarement de la prouesse numérique, mais plutôt du savoir-faire dans l'art de l'illusion.

Au plus haut niveau, les techniques peuvent être combinées et la prouesse technique jointe à l'artifice. Ainsi, certains réseaux ont réussi à insérer des pages de hameçonnage au sein même du site [25] que ces pages sont censées imiter. Concernant eBay et PayPal par exemple, l'imitation est « presque » parfaite. Tout est fait pour cacher l'identité réelle du domaine à l'œuvre. Si vous cliquez sur les liens, vous êtes automatiquement redirigé vers un exécutable qui, selon le rôle et l'intérêt que vous présentez, vous proposera soit un site à l'image du hameçon, soit d'installer un programme qui tournera sur votre machine à d'autres fins.

Avec un peu d'expérience, il n'est certes pas possible de se laisser prendre. Les noms de domaine sont déguisés, même si le pied de message comporte des liens tout à fait réguliers. Ainsi sur le spam-phishing (figure 1) imitant


Please Re-activate your account.
Google AdWords-noreply [adwords-noreply@google.com]
À: [redacted]

Dear Advertiser,

We were unable to process your payment.
Your ads will be suspended soon unless we can process your payment.
To prevent your ads from being suspended, please update your payment information.

Please sign in
to your account at http://adwords.google.com/select/login,
and update your payment information.

Blocked::http://www.adwords.google.com.dikeop.cn/select/Login

We look forward to providing you with the most effective advertising available
Thank you for advertising with Google AdWords.

The Google AdWords Team

Figure 1 - Un spam - phishing visant à introduire des pages phishing de second rang dans des sites normalement hors de tout soupçon.

(21) Ce kit « Rock Phish », du hameçonnage en béton, permet de créer de fausses pages ou de faux messages, ou aspire les vraies pages censées tromper l'internaute.

(22) Là encore, il serait bien illusoire de les appeler des hackers !

(23) Ce qui relève de la publicité mensongère. Les protections sont le plus souvent efficaces, mais elles ne peuvent prétendre combattre toutes les menaces potentielles.

(24) Trop d'informations nuisent à l'information (Syndrome dit de l'Air Bus). Trop de messages préventifs contribuent à fatiguer et à endormir l'usager, ce que précisément recherchent ces spammeurs de haute voltige (« spear phishing » ou hameçonnage de pointe).

(25) Des cas récents (2007, 2008) sont souvent cités et concernent même des sites publics (Grande-Bretagne, Italie notamment).

un message de Google AdWords, si le lien semble tout à fait correct vers adworks.google.com, en fait il conduit vers adwords. google.com.dikeop.cn ou adwords.google.com. coail.cn ! Le site est donc celui de coail.cn et non celui de Google. Mais, quand la souris passe rapidement sur le lien, l'œil croit reconnaître l'identité de Google et vous risquez de ne pas percevoir la supercherie. Un tour sur un des multiples sites capables d'extraire les informations des registres internationaux (*registrars*) permet de constater que ce domaine est enregistré [26] par un certain « hrthh-tfhrthv » (!) On peut lire de plus que cette personne est passée par l'intermédiaire d'un serveur de domaine chinois et qu'il a fait enregistrer pour son compte 320 autres domaines. Inutile de préciser que les outils (non publics ou payants) du même type permettent de tracer sans difficulté ces 320 comptes [27]. Ce domaine a été créé le jour même où nous avons nous-mêmes reçu le spam. Bien des leçons pourraient être tirées de ce simple exemple pris au hasard des messages d'une adresse ordinaire. Il relativise les efforts qui peuvent être entrepris à l'échelle nationale sans coopération internationale. Il est clair que la traque de ces vrais cybercriminels atteindrait vite ses objectifs si les États imposaient le respect des règles. D'un côté, le réseau est mondial, mais de l'autre, le monde est un nid de repères où règne le non-droit, sans qu'il y ait besoin d'aller chercher ici quelque pavillon de complaisance dans de petits États qui, au contraire, semblent plutôt jouer le jeu.

Aussi, les moyens mis en œuvre, pour ces raisons, atteignent la moyenne et la petite délinquance plutôt que les nouvelles mafias, dont les relations avec certaines des « nouvelles » puissances mériteraient d'être étudiées de plus près. Courons-nous un risque en écrivant cela ? Le site des *Cahiers de la sécurité* a lui-même été attaqué par un virus exploitant les failles du système de base de données SQL. C'était mal fait et ce fut vite repéré et sans conséquence. Mais, il est clair qu'il y a deux batailles.

Les responsables de ces attaques restent pour la plupart du temps impunis. Quelques-uns se sont fait prendre, souvent du fait de l'inexpérience d'un ou de deux complices opérant sur des réseaux à petite échelle. À l'échelle qui nous intéresse ici, celle de la criminalité organisée, il faut reconnaître que les prises sont maigres et ne concernent pas l'étage supérieur des organisations mafieuses. D'où d'ailleurs la difficulté à décrire dans le détail la réalité de leur fonctionnement. Beaucoup de lignes sont écrites et peu correspondent à la réalité.

Mais les États sont contraints de s'intéresser à la sécurité des réseaux, car elle devient un enjeu important. Des États ont ainsi accusé la Chine d'avoir attaqué des sites stratégiques. Le hacking est devenu une industrie de série pour les mafias, il est en passe de devenir un instrument discret, sophistiqué et de pointe pour la guerre économique et celle du renseignement. L'Estonie, attaquée de toute part, a dû isoler ses réseaux pendant deux jours et demander l'intervention de l'OTAN pour la protéger des attaques supposées de la Russie. La situation actuelle de la Géorgie a été influencée par ce type de conflit. Deux sortes d'attaque peuvent être menées, celle qui consiste à intercepter des informations et celle qui vise à créer un chaos subit. Aussi, la guerre conventionnelle tendra à se doubler de plus en plus d'une guerre numérique. Sur ce point encore, les catastrophes naturelles, dont les crises sont gérées par les autorités de la sécurité civile, convergent vers les situations que peut créer une guérilla numérique. Si l'on excepte les couches les plus critiques des applications militaires (dont le coût – relatif- est de ce fait sans cesse croissant), les systèmes informatiques utilisés par les infrastructures critiques [28] sont fondés sur les couches les plus répandues des systèmes de communication numérique. Parce qu'ils sont clairement plus efficaces et moins onéreux que des systèmes propriétaires que seuls peuvent – ou doivent [29]- s'offrir quelques industries de pointe, comme les industries militaires ou nucléaires. Une large diffusion crée la menace. Ainsi, les logiciels dits libres ou minoritaires (comme Apple) n'ont acquis la réputation d'être plus « sécurisés » que parce qu'ils sont moins soumis aux attaques. Ils présentent d'autres types de danger.

En fait, tous les États (sauf peut-être la France, la Suisse et la Suède ?) attaquent leurs partenaires pour renforcer leurs positions et celles de leurs entreprises. Certes, certains pays comme la Chine ne cachent rien de la réalité de ce

••••

(26) Recherche réalisée le 31 août 2008 sur le moteur d'extraction du site http://whois.domaintools.com/ alors que le message a été reçu une semaine auparavant, le 24 août, par des milliers sinon des millions de personne... Cela donne une idée du mur auquel les polices se heurtent dans leur combat contre ces mafias alors que l'envoi d'une centaine d'e-mails individuels sur un serveur d'un des plus grands pourvoyeurs d'adresses mail vous « blackliste » temporairement mais immédiatement...

(27) En utilisant un autre outil à la disposition de tous, il apparaît que le serveur de ces domaines est localisé à... Stuttgart. Autre particularité de ce message : il est envoyé depuis l'adresse usurpée du destinataire qui n'aura donc pas la possibilité de la déclarer comme indésirable.

(28) Réseaux d'approvisionnement et de traitement des eaux, systèmes de détection des incendies, les centrales, les systèmes de gestion des transports et de la circulation, les barrages... et même les réseaux de pilotage des crises.

(29) En 2003, un « ver » a paralysé le réseau de surveillance d'une centrale nucléaire américaine (l'obligation de résultat plus que de moyens peut, dans ce domaine, comporter des conséquences inattendues).

combat si bien qu'une culture du hacking a gagné les milieux mafieux qui accompagnent leur formidable décollage économique. Un phénomène semblable s'est produit en Russie où les services de renseignement recrutent les meilleurs ingénieurs informatiques qui sortent des écoles. Mais, le « sale boulot » est confié aux prestataires sans vouloir voir qu'ils sont également au service des mafias. Si les mafias sont poursuivies, les prestataires de service sont relativement épargnés. Tous ces milieux sont liés. Et la question se pose, lancinante, de savoir s'il est possible de lutter contre les menaces émergentes qui nous concernent sans, quelque part, pactiser avec le diable. C'est le pari légitime qui sous-tend le plan français (*cf.* encadré). Mais, alors, il faudra y mettre les moyens car ces cybercriminels n'ont rien de la bande à Bonnot.

2008 : un plan officiel contre la cybercriminalité

Ce plan a été présenté en février 2008. En fait, le pivot de la lutte contre la cybercriminalité en France se situe à l'OCLCTIC, l'Office central de lutte contre la criminalité liée aux techniques de l'information et de la communication. Dépendant de la direction centrale de la Police judiciaire (DCPJ), l'OCLCTIC est l'interlocuteur privilégié du gouvernement et représente la France lors des réunions étrangères. Il a été créé en mai 2000 et s'est largement appuyé sur les méthodes virales en vigueur dans les années 1995-99. Il compte une cinquantaine de personnes regroupées en trois sections principales. La première rassemble des enquêteurs habilités à faire un travail de police sur tout le territoire et à l'étranger. La deuxième est une section technique (veille, formation). La dernière gère la plate-forme de signalement.

Comme le reconnaît lui-même Christian Aghroum [30], chef de l'OCLCTIC, la cyber-délinquance a beaucoup évolué. Nous sommes sortis de l'ère des pionniers. L'Internet ressemble finalement à la société. D'un côté du triangle, les voleurs à la tire utilisent le réseau et les recettes virales (ou non virales) qu'il est aisé de trouver sur Internet pour extorquer de l'argent aux usagers les plus crédules. D'un autre côté, des pirates organisés attaquent des sites, des processus où transitent des données sensibles afin de voler identifiants, données monnayables ou secrets de fabrication. Sur le troisième pilier, innovation et « hackage » se donnent la main sans relation directe avec la délinquance, celle allant de la délinquance simple au grand banditisme criminel et à l'instrumentalisation par des organisations mafieuses nouvelles ou reconverties, voire par des organisations terroristes.

La qualification criminelle de ces délinquants relève de niveaux très différents. Les détecter puis les poursuivre constituent des métiers différents. De fait, les 500 enquêteurs dont disposent la police et la gendarmerie à ces fins, sont répartis dans différents services. Le dispositif a dû difficilement suivre le rythme de l'évolution et de la diversification de la délinquance. La ministre de l'Intérieur a donc légitimement voulu adapter l'effort de l'État par une remise à plat du dispositif en programmant le doublement des effectifs des enquêteurs spécialisés d'une part, et en renforçant le rôle pivot de l'OCLCTIC d'autre part. L'office se concentrerait sur la délinquance qui demande une coopération internationale renforcée, assurerait une veille technologique, et partant, constituerait le référent expert des nouvelles technologies utilisées à des fins délinquantes et assurerait les formations des enquêteurs spécialisées.

D'autres mesures sont proposées par ce plan pour accompagner cette évolution :

- la création d'un cursus spécialisé au sein de la Police nationale ;
- l'extension de la plateforme de signalement des communications xénophiles et pédophiles à toutes les formes d'escroquerie et de terrorisme en ligne ;
- la mise à disposition des policiers d'outils de captation de données à distance ;
- la création d'un site de référence pour les internautes [31] ;
- l'obligation de conserver les données de connexion utiles à l'identification des créations de contenu ;

(30) Se reporter à l'article de Christian Aghroum dans ce numéro.
(31) Pour l'heure, le site est à cette adresse : http://www.interieur.gouv.fr/sections/contact/police/questions-cybercriminalite

- la création d'un délit d'usurpation d'identité sur internet (jusqu'à un an d'emprisonnement et 15 000 euros d'amende) ;

- l'utilisation des compétences des « hackers » condamnés pour les utiliser au service de la collectivité, en créant une nouvelle peine alternative (type de sanction existant déjà à l'étranger et d'efficacité relative tant les compétences de ces hackers relèvent parfois du mythe).

En fait, cette volonté amorce un effort pour prendre en compte progressivement la différenciation qui s'est opérée. Entre la blague potache qui consiste à usurper l'e-mail d'un ami sur MSN, la délinquance de proximité (diffuser des photos volées par exemple) et organiser un réseau de robots rabattant des données escroquées et monnayables sur une grande échelle, il y a une différence dans le niveau du délit et la qualification criminelle. Le problème est que, contrairement à l'idée reçue, les outils sont souvent les mêmes et pis, les outils de l'Internet permettent ces escroqueries mineures ou majeures sans aucun recours à des malwares [32] ; il est à la portée de tout utilisateur d'envoyer un e-mail en empruntant l'identité d'un tiers...

Nous voilà revenus à la case départ de la délinquance ordinaire. Faut-il mettre sous surveillance tous les tournevis au motif qu'ils peuvent servir à crocheter une porte... Il est possible de demander aux opérateurs comme aux hébergeurs de conserver toutes les données susceptibles d'identifier [33] les poseurs [34] de contenu en ligne. Cela ne nous conduira pas vers la société de « big brother » contrairement à ce qui est souvent avancé. En revanche, cela risque de conforter les risques et de déporter les menaces. S'il s'agit de la petite délinquance, il est envisageable de demander aux hébergeurs de réaliser un minimum de « flicage ». Ce n'est en réalité ni plus ni moins que du ressort de l'éthique. Mais, cela ne règle pas la question des organisations criminelles mafieuses car, le plus souvent, ils contrôlent leurs hébergeurs centraux dans des États qui, souvent, les tolèrent. Encore une fois, ce n'est pas une question d'outil. Usurper l'identité d'un e-mail pour faire une blague et créer un robot qui utilise la même technique reproduite des millions de fois pour escroquer ne peut relever de la même approche. De la civilité ordinaire et de ses manquements à l'attentat criminel à l'ordre public, il y a une marge que les décrets prévus par le plan Alliot-Marie vont devoir apprécier. En clair, la cybercriminalité ne peut être traitée isolément des questions qui relèvent de la sécurité globale, civile, certes, mais aussi économique (question de l'intelligence économique et/ou territoriale), mais aussi militaire.

Patrice HERNU

DOSSIER

....

(32) Softwares (logiciels) malicieux.

(33) Adresse IP, mot de passe, identifiant, machine utilisée, etc.

(34) « Créateurs » est un bien grand mot pour ce qui effectivement transite par ces canaux !

DOSSIER

Combattre le cybercrime

Un point de vue du ministre de la Justice de l'État de Washington

Rob McKENNA

Dans le monde entier, des entités privées et publiques ont été mises au défi de développer rapidement de nouvelles techniques afin de faire face au « cybercrime ». Le ministère de la Justice de l'État de Washington est reconnu comme un leader national pour ses efforts dans la lutte contre la criminalité « high-tech ». L'État de Washington a été l'un des premiers à adopter une loi interdisant explicitement les activités de logiciels espions (« spyware ») et à imposer des peines sévères à ceux qui l'enfreindraient. Le succès de cette entreprise dépend d'une législation bien ficelée, de ressources adéquates, de partenariats, d'un soutien aux forces de police, et de l'information dispensée aux consommateurs et aux entreprises.

Fighting Cybercrime
A Perspective from the Washington State Attorney General

Throughout the world, public and private entities have been challenged to quickly develop new techniques to address cybercrime. The Washington State Attorney General's Office is known as a national leader in efforts to fight high-tech crimes. Washington was one of the first states to adopt a law explicitly prohibiting spyware activities and imposing serious penalties on violators. Success depends on well-crafted legislation, adequate resources, partnerships, support for law enforcement, and consumer and business education.

Rob McKenna

Rob Mc Kenna a été élu 17e ministre de la Justice de l'État de Washington et a pris ses fonctions en 2005. Il a commencé sa carrière de juriste en 1988 chez Perkins Coie, l'un des cinquante meilleurs cabinets d'avocats des États-Unis. Il a obtenu son diplôme d'avocat à l'université de Chicago (*University of Chicago Law School*), est titulaire de deux licences en économie et études internationales. Il est membre du *Aspen-Rodel Fellowships in Public Leadership*, association conçue dans le but de réunir les meilleurs dirigeants qui commencent à se distinguer dans le pays, pour discuter des grandes questions de la gouvernance démocratique et d'un service public efficace.

© Cahiers de la sécurité -INHESJ

Tandis qu'Internet a révolutionné la manière de communiquer et de conduire ses affaires pour bon nombre de personnes, il a aussi favorisé une augmentation gigantesque de la criminalité exploitant cette technologie. Dans le monde entier, les entités publiques et privées ont été mises au défi de développer rapidement de nouvelles techniques pour faire face au cybercrime, qui va de la fraude financière à la diffusion de logiciels malveillants et destructeurs (*destructive malware*), en passant par l'exploitation des enfants, le harcèlement et le vol de secrets commerciaux.

L'augmentation du cybercrime

75 % des adultes et 90 % des enfants, estime-t-on, utilisent Internet [1] aux États-Unis. Avec un tel nombre de familles, d'entités gouvernementales et d'entreprises en ligne, l'essor correspondant du cybercrime représente une sérieuse menace pour la sécurité publique, l'économie et la sécurité nationale.

L'impact réel du cybercrime aux États-Unis demeure inconnu, car les incidents ne sont pas toujours signalés ou détectés. Les études disponibles révèlent une augmentation substantielle de l'activité illégale, qui comporte :

- Les spams : la société Postini a repéré plus de 60 milliards de spams entre septembre 2006 et mars 2007. La société a relevé une augmentation de 65 % de spams depuis janvier 2002 [2] ;

- Les ordinateurs infectés par des bots (robogiciels) : la Symantec a relevé 63 912 ordinateurs infectés chaque jour pendant cinq mois en 2005, soit une augmentation de 11 % par rapport à la précédente période étudiée [3] ;

- Les attaques d'un cheval de Troie : 2 millions sur les 4 millions d'ordinateurs nettoyés par un outil de suppression de logiciels malveillants de Microsoft, entre janvier et juin 2006, étaient infectés par au moins un cheval de Troie déguisé. Durant le même laps de temps, 43 000 nouvelles variantes de logiciels malveillants ont été découvertes. Le secteur des services financiers a été victime de presque 40 % de toutes les attaques de chevaux de Troie l'année dernière, selon Counterpane [4].

- Espions clavier enregistreurs de frappe (*Keyloggers*) : Le Groupe de travail contre les faux courriels ou pages web (*Anti-Phishing Working Group* - APWG), une association d'entreprises informatiques, a rapporté que le nombre de sites hébergeant des enregistreurs de frappe criminels (*keylogging crimeware*) s'élevait à 3 362 en janvier 2008. [5]

- Faux courriels ou pages web : APWG a détecté 299 307 URLs uniques durant l'année 2007, et a noté que les États-Unis restent le premier pays hébergeant des sites d'hameçonnage avec 37 % du total de ce genre de sites. Plus de 55 % des attaques d'hameçonnage sont des contrefaçons de sites internet d'entreprises hébergées aux États-Unis, selon un rapport d'IBM. [6]

- Les virus : 38 % des individus interrogés par « *Consumer Report* » ont fait État d'une infection de leur ordinateur par un virus durant ces deux dernières années, et 34 % ont signalé une infection par un logiciel espion durant les six derniers mois. Les infections par virus ont incité 1, 8 million de foyers à remplacer leurs ordinateurs personnels ces deux dernières années, et 850 000 les ont remplacés ces six derniers mois en raison d'infections par des logiciels espions. [7]

Les entreprises, autant que les usagers, sont victimes de cette criminalité :

- le Centre de plaintes pour crimes sur Internet (*Internet Crime Complaint Center*) a totalisé plus de 90 000 plaintes auprès des services de police en 2007, qui s'élèvent à des pertes de près de 239,09 millions de dollars [8];

- les consommateurs américains ont perdu une somme estimée à 7,2 milliards de dollars en raison de virus, logiciels espions et hameçonnage en 2006 [9];

••••

(1) *Pew Internet and American Life Project*, février 2008, www.pewinternet.org

(2) «Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats», GAO-07-705, U.S. *Government Accountability Office*, juin 2007, www.gao.gov

(3) *Idem*.

(4) *Idem*.

(5) «Phishing Activity Trends -January 2008», *Antiphishing Working Group*, www.antiphishing.org

(6) *Op. cit.*, www.gao.gov

(7) «2007 State of the Net report», Consumers Reports, http://www.consumerreports.org

(8) «2007 Internet Crime Report», *Internet Crime Complaint Center*, www.ic3.gov, La création de ce centre est le résultat du partenariat entre le *Federal Bureau of Investigation* (FBI), l'association à but non lucratif *National White Collar Crime Center* et le *Bureau of Justice Assistance*.

(9) «2007 State of the Net report», *Consumers Reports*, http://www.consumerreports.org

© Cahiers de la sécurité -INHESJ

- les organisations américaines ont perdu une somme estimée à 67,2 milliards de dollars en raison de la criminalité informatique en 2005 [10];

- une enquête auprès d'entreprises américaines a montré que les pertes moyennes annuelles dues au cybercrime ont plus que doublé, passant de 168 000 dollars en 2006 à 424 000 dollars en 2007 [11].

La mise en réseau des ordinateurs a aussi ouvert la voie à des types de criminalité qui menacent la sécurité publique, comme le harcèlement et l'exploitation des enfants.

- une enquête récente [12] a montré qu'un enfant sur sept ayant entre 10 et 17 ans a reçu une sollicitation sexuelle en ligne ; un sur trois s'est trouvé involontairement exposé à des photos de personnes nues ou d'activités sexuelles ; et un sur onze a été menacé ou harcelé ;

- d'autres recherches ont montré que 7 % des jeunes adolescents utilisateurs du Net disent avoir eu peur ou s'être sentis mal à l'aise à la suite d'un contact en ligne avec un inconnu [13];

- des responsables gouvernementaux ont annoncé en juillet 2007 que MySpace.com a recensé, sur son site internet en réseau très en vogue, plus de 29 000 délinquants sexuels fichés par les services de police.

Patrouiller dans le cyberspace

De nombreux organismes aux États-Unis ont pour mission de détecter, enquêter et poursuivre en justice le cybercrime. Les acteurs clefs à l'échelon du gouvernement fédéral sont le ministère de la Justice, de la Sécurité intérieure, de la Défense, et la Commission Fédérale du Commerce. Les polices, à l'échelon local et à celui des États, jouent aussi un rôle important en matière de protection de la population.

En tant que premiers magistrats de la hiérarchie judiciaire de chacun des États fédérés, les ministres de la Justice exercent une fonction de conseillers auprès des organes législatifs et exécutifs, et jouent aussi le rôle de procureur général au service de tous les citoyens. Bien que variant d'une juridiction à l'autre en raison des dispositions constitutionnelles et statutaires de chaque État, leurs pouvoirs habituels consistent à faire appliquer les lois de leur État fédéré ; agir en tant que défenseurs des intérêts publics dans des domaines tels que la protection de l'enfance, la protection des consommateurs, la régulation antitrust et des services publics ; proposer des lois ; et porter la responsabilité de représenter le gouvernement de l'État lors des procès.

Le ministère de la Justice de l'État de Washington est reconnu comme un leader national en matière d'efforts pour combattre les crimes high-tech. En 2000, l'État de Washington est devenu le deuxième État fédéré en matière d'innovation dans ce domaine. Le ministère de la Justice de l'État a développé une unité entièrement spécialisée dans la protection des consommateurs victimes de criminalité high-tech [14]. Il propose aussi une législation permettant d'épauler la police et les juges d'instruction dans leur travail, fournit une formation aux résidents de l'État de Washington afin de les prémunir contre le cybercrime, et construit des partenariats efficaces avec différents organismes qui travaillent à combattre cette menace.

Peu de temps après avoir gagné mon élection au poste de ministre de la Justice en 2005, j'ai recherché un appui supplémentaire auprès des assemblées législatives de notre État afin de faire face à l'augmentation vertigineuse de la fraude high-tech et des affaires de vols d'identités dans notre État. Les deux chambres ont approuvé une rallonge budgétaire de 1,6 million de dollars pour notre Bureau de protection du consommateur, dont une partie a pu financer deux nouveaux experts juridiques, un expert en analyses d'ordinateurs, ainsi qu'un laboratoire informatique de pointe où des outils sophistiqués sont utilisés pour détecter les hackers, les pourvoyeurs de logiciels espions et d'autres types de fraudes sur Internet.

....

(10) «2005 Computer Crime Survey», FBI.

(11) «2007 Computer Crime and Security Survey», *Computer Security Institute*, www.gocsi.com

(12) «Online Victimization: A Report on the Nation's Youth», 2006, *National Center for Missing and Exploited Children* (Centre National pour les Enfants exploités ou Disparus), www.missingkids.com

(13) «Teens and Online Stranger Contact», octobre 2007, *Pew Internet and American Life Project*, www.pewinternet.org

(14) Le combat du ministre de la Justice de l'État de Washington (*Washington Attorney General*) contre le cybercrime se déroule essentiellement dans le domaine du droit civil, dans lequel les sanctions comprennent des amendes pour les contrevenants et des dispositions injonctives qui rendent obligatoires des changements dans les pratiques commerciales. Si les ministres de la Justice de certains États fédérés ont autorité pour engager des poursuites judiciaires pour des affaires criminelles qui peuvent entraîner l'emprisonnement, la législation de l'État de Washington limite l'autorité du ministère pour enquêter et poursuivre de telles affaires en justice criminelle. Le ministère n'ouvre pas d'enquêtes criminelles sans une requête de la part du procureur d'un comté ou du Gouverneur.

© Cahiers de la sécurité -INHESJ

Éliminer les « spyware »

Le spyware [15] est manifestement devenu la plus importante menace en ligne pour les consommateurs et le monde des affaires depuis l'existence d'Internet. L'État de Washington a été l'un des premiers à adopter une loi interdisant explicitement les activités de spyware et prévoyant de lourdes sanctions à l'encontre de ceux qui l'enfreindraient.

La Loi de l'État de Washington sur les Logiciels Espions des Ordinateurs (*Washington Computer Spyware Act* [16]) a pris effet en juillet 2005, et donne au ministère de la Justice un puissant instrument pour décourager et poursuivre en justice les pourvoyeurs de spyware. Le ministère de la Justice a obtenu des jugements favorables aux consommateurs dans la totalité des six poursuites en justice déjà intentées.

Treize États fédérés ont maintenant adopté une législation qui combat spécifiquement le spyware. La nécessité d'un tel dispositif est rendue évidente si on se reporte aux statistiques stupéfiantes, y compris les rapports qui estiment que le spyware et d'autres logiciels indésirables sont installés sur 80 % des ordinateurs des usagers [17]. Une étude réalisée par des fournisseurs de logiciels a trouvé une moyenne de vingt-cinq logiciels espions, logiciels publicitaires (« adwares ») et autres programmes potentiellement indésirables par ordinateur personnel [18]. Microsoft a relevé que 50 % de ses demandes d'assistance informatique de la part de ses utilisateurs confrontés à des pannes d'ordinateurs provenaient de spywares.

Tandis que s'accroissent les inquiétudes sur la sécurité informatique, la confiance du consommateur dans le commerce et les transactions financières en ligne est susceptible d'être ébranlée. La seule manière de préserver la fiabilité du marché Internet est, du point de vue du ministère de la Justice, d'aborder les procès high-tech comme n'importe quels autres et d'exercer ses pouvoirs de police au moment opportun.

Dans leur combat contre le spyware, les États rencontrent un problème majeur, à savoir la confusion très répandue et la controverse sur les définitions du spyware par opposition à l'adware. Certains pensent qu'un logiciel qui ramasse la moindre information sur l'usage d'un ordinateur par son utilisateur devrait être appelé spyware. D'autres considèrent qu'un logiciel intégré affichant de la publicité ciblée est un spyware. D'autres encore pensent que la définition devrait être limitée au logiciel qui vole des informations personnelles.

La loi de l'État de Washington sur les spyware définit celui-ci par les effets du logiciel sur l'ordinateur d'un utilisateur, ainsi que par la méthode selon laquelle il a été installé. La loi interdit de recueillir des informations personnelles identifiables par le biais de l'espionnage qui surveille la frappe sur le clavier (enregistreurs de frappe) ; de collecter l'historique de la navigation d'un usager sur le Net ; de prendre le contrôle d'un ordinateur personnel pour envoyer des courriels non autorisés ou des virus ; de créer de fausses charges financières ; d'orchestrer des attaques groupées sur d'autres ordinateurs ; d'ouvrir des « pop-ups [19]» ; de modifier les paramètres de sécurité ; et d'interférer avec la capacité de l'utilisateur à identifier et enlever le spyware.

La loi de l'État de Washington sur les spyware ne se limite pas à proscrire les programmes qui répondent à la définition la plus étroite de ce dernier, mais punit aussi ceux qui font des présentations faussées pour inciter les utilisateurs à installer un logiciel, y compris les présentations trompeuses quant à l'efficacité de la protection assurée par un logiciel de sécurité sur un ordinateur personnel.

Le ministère de la Justice – ou tout possesseur d'un site web ou d'une marque de fabrique qui est victime de piratage par spyware – peut intenter une poursuite en justice en invoquant notre loi. Microsoft l'a fait avec beaucoup de succès. Les accusés peuvent être condamnés jusqu'à 100 000 dollars d'amende pour infraction ou à hauteur de l'évaluation des dommages subis, et un tribunal peut même relever le seuil des dommages à hauteur d'un maximum de 2 millions de dollars. Une infraction à la loi sur les spyware est aussi une infraction à la loi de l'État de Washington sur la protection du consommateur [20], au terme de laquelle les contrevenants peuvent être condamnés à une amende pouvant s'élever jusqu'à 2 000 dollars par infraction.

(15) Globalement, le spyware est un logiciel trompeur installé dans un ordinateur, souvent à l'insu de l'usager ou sans son consentement en connaissance de cause. Un tel logiciel peut collecter et transmettre des informations personnelles, modifier d'importantes configurations de confidentialité et de sécurité, et même prendre totalement le contrôle de l'ordinateur de l'usager.

(16) *Revised Code of Washington* (RCW) 19.270, www.leg.wa.gov

(17) Enquêtes réalisées en 2004 par l'Institut d'études de marchés IDC et le *National Cyber Security Alliance*.

(18) *Earthlink and Webroot Software's SpyAudit*, rapport rendu public en février 2005.

(19) Fenêtre intruse ou fenêtre surgissante de publicités agressives dans une fenêtre secondaire qui s'affiche sans avoir été sollicitée par l'utilisateur devant la fenêtre de navigation principale lorsqu'on navigue sur Internet.

(20) RCW 19.86, www.leg.wa.gov

© Cahiers de la sécurité -INHESJ

Le ministère de la Justice a intenté six procès fondés sur notre loi contre les Spyware. Ces poursuites judiciaires ont eu pour objet une variété d'itérations de spywares, et ont toutes entraîné des décisions comprenant des dommages et intérêts, des injonctions à cessation immédiates des activités incriminées, et le dédommagement des consommateurs lésés. Les exemples sont les suivants :

- En janvier 2006, nous avons intenté notre premier procès contre *Secure Computer*, installé à New York, un supposé vendeur de produits anti-spyware, qui faisait de la publicité par le biais de « pop-ups » (fenêtre intruse ou fenêtre surgissante) qui déformaient le risque, pour l'utilisateur, d'une infection par spyware. Le pop-up, qui ressemblait à une alerte officielle de sécurité de Microsoft, encourageait l'utilisateur à mettre en place un scan gratuit de l'ordinateur. Le scan montrait toujours la présence d'un spyware, même s'il n'y en avait aucun. Les pop-ups ne pouvaient pas être fermés en cliquant sur les points de fermeture habituels. Une issue au procès fut finalement trouvée avec tous les accusés par un dédommagement d'un million de dollars aux consommateurs.

- En août 2006, le ministère de la Justice de l'État de Washington a poursuivi *Digital Enterprises d/b/a/Movieland.com*, accusé d'offrir des abonnements avec essais gratuits à des films pour adultes, pour ensuite facturer les particuliers en leur envoyant d'incessants pop-ups sous forme de vidéos, leur réclamant un paiement après l'expiration de la période d'essai. Les destinataires se trouvaient dans l'incapacité de fermer ou réduire les pop-ups. L'État de Washington allégua que *Movieland* avait installé le spyware à l'origine de la présentation répétitive de la vidéo, et de sa réinstallation automatique, même lorsque l'usager tentait de la désinstaller. L'affaire s'est réglée par une injonction obligeant les accusés à cesser de faire de la publicité par le biais de cette méthode, le paiement d'indemnités et le dédommagement des consommateurs.

- En octobre 2006, nous avons poursuivi *High Falls Media* et *ROC Telecommunications* pour leur logiciel « Spyware Slayer » qui incitait, de manière frauduleuse, les utilisateurs à l'installer en prétendant faussement que leurs ordinateurs étaient prétendument déjà infectés. L'affaire s'est réglée par une injonction limitant à l'avenir ces pratiques publicitaires, et le paiement d'indemnités ainsi que le dédommagement des consommateurs.

- En novembre 2006, nous avons poursuivi un particulier de New York à propos de son logiciel « QuickShield » qui incitait les usagers à l'installer en faisant de fausses évaluations de leurs vulnérabilités en matière de sécurité. L'affaire s'est réglée encore une fois par une injonction de cessation, le paiement d'indemnités et le dédommagement des consommateurs.

- En février 2007, l'État de Washington a poursuivi *Securelink Networks* et LLC, installés en Californie, et plusieurs autres accusés, pour l'utilisation de messages « Net Send » et des scans gratuits trompeurs pour vendre leurs produits (Registry Sweeper Pro, Registry Rinse, Registry Doc, Registry Cleaner 32 et Registry Cleaner Pro). Les messages induisaient les utilisateurs en erreur en leur faisant croire que leurs ordinateurs étaient infectés, et qu'il leur fallait acheter les produits en question afin de les nettoyer. Le tribunal accepta les requêtes de l'État de Washington qui réclamait un jugement immédiat, ordonnant aux accusés de rembourser des centaines de consommateurs de l'État de Washington.

- En mars 2008, nous avons poursuivi un particulier, à Scottsdale en Arizona, pour avoir contraint les usagers à acheter un logiciel bloquant les pop-ups de leur ordinateur en les bombardant préalablement de publicités pour le Viagra, et d'autres de nature pornographique. Notre plainte alléguait que les usagers qui téléchargeaient les produits vantés par la publicité, qui comprenaient Messenger Blocker, WinAntiVirus Pro 2007, System Doctor et WinAntiSpyware, subissaient un préjudice supplémentaire quand le logiciel provoqua l'envoi massif et furtif de messages, à partir de leurs propres ordinateurs, vers d'autres ordinateurs personnels, à un rythme d'un toutes les deux secondes. L'affaire s'est réglée en mai 2008 par une injonction de cessation et le dédommagement des usagers lésés.

À l'échelon fédéral, l'accès non autorisé à un ordinateur est illégal, aux termes de la loi *Computer Fraud and Abuse Act* [21]. Les législateurs fédéraux ont tenté en vain, à partir de 2004 et plus récemment en 2007, de voter une loi pénalisant plus sévèrement les créateurs de spyware en augmentant les peines de prison. La loi établissant la Commission au commerce fédéral (*Federal Trade Commission Act* – FTCA) fournit des dispositions facilitant les poursuites contre les fournisseurs de spyware. Bien que le FTCA ne soit pas aussi précis que le *Computer Spyware Act* de l'État de Washington dans la définition des pratiques frauduleuses, il s'est avéré assez efficace dans de nombreuses poursuites judiciaires fédérales.

(21) 18 U.S.C. § 1030, http://www.gpoaccess.gov/USCODE/index.html

© Cahiers de la sécurité -INHESJ

Réduire les spams

À vrai dire, le ministère de la Justice de l'État de Washington a combattu le crime high-tech depuis plus de dix ans, et a fait date en octobre 1998 en lançant la première poursuite en justice d'un État fédéré contre un pourvoyeur d'e-mails non sollicités (« spammer »).

La loi de l'État de Washington contre les courriers électroniques commerciaux indésirables (*Unsolicited Commercial Act*) [22], entrée en vigueur un peu plus tôt cette année-là, a été une des premières dans le pays à réglementer l'envoi de spams. Elle interdit l'envoi de courriels commerciaux indésirables et contenant des informations mensongères, qui utiliseraient le nom de domaine d'un tiers sans autorisation, ou déformeraient le point d'origine du message. La loi impose des pénalités qui peuvent aller jusqu'à 500 dollars par courriel.

Notre poursuite judiciaire accusait un résident de l'Oregon, Jason Heckel, d'avoir envoyé des spams à des millions d'utilisateurs d'Internet pour vendre sa brochure en ligne, intitulée « Comment tirer un avantage d'Internet ». La Cour suprême de l'État de Washington a confirmé, en 2001, la constitutionnalité de notre loi de l'État contre les spams. La Cour suprême fédérale a refusé de réexaminer l'affaire, rendant impossible tout appel de la part de Heckel.

Les assemblées ont amendé la loi anti-spam de notre État en 2005, pour interdire spécifiquement les faux e-mails ou fausses pages web dans lesquels l'identité falsifiée des voleurs induit les consommateurs en erreur. Ces e-mails, qui semblent provenir d'une entreprise, d'une banque ou d'un site de vente aux enchères en ligne, extorquent des informations personnelles. La loi rend illégal le fait qu'une personne travestisse son identité dans le but de solliciter ces informations en ligne.

Le Congrès fédéral a voté la loi *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act* [23] en 2003, interdisant les e-mails faux ou trompeurs et exigeant que les auteurs de la publicité laissent aux destinataires la possibilité de refuser des sollicitations ultérieures.

Le ministère de la Justice de l'État de Washington a entrepris sa première poursuite en justice en invoquant cette loi peu de temps après son entrée en vigueur en 2004. Le procès intenté, instruit à l'*U.S. District Court*, alléguait que AvTech Direct, une entreprise de marketing californienne maintenant disparue, et MD&I, une société de vente d'ordinateurs installée en Californie, utilisaient des annonces trompeuses et faisaient croire que les messages provenaient d'autres sources.

Stopper la publicité mensongère sur Internet

Le ministère de la Justice de l'État de Washington a porté devant les tribunaux plus d'une douzaine d'affaires impliquant la publicité sur Internet depuis 2005. Au-delà de notre législation sur les spyware et les spams, la loi de l'État de Washington « *Unfair Business Practices-Consumer Protection Act* » [24] nous donne un large pouvoir de réglementation. La législation interdit les pratiques déloyales ou trompeuses en matière commerciale et autorise le ministère à réclamer des amendes pouvant aller jusqu'à 2 000 dollars par infraction.

Très récemment, nous avons pris des mesures répressives à l'encontre de publicitaires affiliés à Internet qui utilisaient des pop-ups Net Send ou Windows Messenger pour commercialiser des logiciels de façon trompeuse. Windows Messenger Service, à ne pas confondre avec le programme de messages instantanés Windows Live Messenger, est essentiellement conçu pour être utilisé sur un réseau et autorise ses administrateurs à envoyer des notices aux usagers. Notre enquête a découvert qu'un nombre croissant d'individus inondait les consommateurs de messages Net Send et de publicités par pop-ups traditionnels qui ressemblaient fréquemment à des systèmes d'alerte. Leur intention était de faire peur aux usagers pour qu'ils achètent un produit supposé protéger leur ordinateur contre les pop-ups, virus et spywares. De nombreux usagers se sont retrouvés en train de payer pour un programme qui n'était quasiment d'aucune utilité ou qui rendait leur ordinateur encore plus vulnérable aux malware. Nos poursuites en justice ont eu pour résultat l'arrêt définitif de nombre de ces opérations et l'obtention de remboursements aux usagers.

Nous avons aussi récemment intenté des poursuites contre des sociétés en ligne qui faisaient la promotion de produits onéreux « gratuits », comme des télévisions à

(22) RCW 19.190, www.leg.wa.gov
(23) U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037, http://www.gpoaccess.gov/USCODE/index.html
(24) RCW 19.86, www.leg.wa.gov

© Cahiers de la sécurité -INHESJ

haute définition, des caméras digitales et des ordinateurs portables. Les consommateurs devaient finalement payer une somme plus élevée que le prix réel afin de les recevoir. Plus encore, nous avons allégué que ces entreprises étaient en fait à la recherche d'informations personnelles concernant les usagers, afin de pouvoir les vendre. Ces poursuites en justice ont eu pour résultat des injonctions interdisant les pratiques de ces sociétés et prévoyant des réparations pour les consommateurs. Nos poursuites en justice ont aussi concerné des pratiques de facturations trompeuses et le non-respect de commandes de marchandises, entre autres affaires.

Promouvoir la sécurité des données

La sécurité des données et la protection des informations personnelles sont devenues des défis juridiques et commerciaux majeurs, tant pour les entités publiques que privées. On estime que les entreprises dépensent chacune une moyenne de 5 millions de dollars pour se remettre d'un incident concernant le non-respect de la sécurité de leurs données. Bien entendu, ces violations ont des effets très néfastes sur la confiance des consommateurs. Par conséquent, le public réclame plus de protections. La sécurité financière est d'une importance primordiale, et il est de notre responsabilité de protéger le public contre les pratiques commerciales qui mettent en danger leur sécurité.

L'État de Washington s'est joint à presque la moitié des États fédérés qui légifèrent sur la violation de la sécurité en ligne pour exiger de la part des entreprises, ainsi que des organes gouvernementaux à l'échelon local et fédéral, qu'ils divulguent les violations de leurs systèmes de sécurité non cryptés contenant des informations personnelles de leurs clients. Aucun organisme répressif n'est spécifiquement désigné pour appliquer notre loi punissant le viol des données personnelles [25], mais le ministre de la Justice peut assumer ce rôle par défaut.

Le but de notre législation est d'assurer que, si un viol de données survient, les usagers en soient rapidement notifiés, afin de leur permettre de s'assurer de la protection de leurs informations personnelles. Notre législation exige que la divulgation d'un non-respect de la confidentialité des données soit faite « *sans retard déraisonnable, compatible avec les besoins légitimes pour appliquer la loi* ». Cela comprend une notification écrite et électronique ou, dans certains cas, la publication d'avertissements dans les médias. La législation encourage les administrations et les entreprises à assumer la responsabilité des données des usagers et à leur permettre d'agir rapidement pour assurer l'intégrité de leurs informations personnelles.

Une autre loi de l'État de Washington [26] exige des entreprises et des administrations publiques qu'elles détruisent les informations personnelles de manière responsable. Les contrevenants engagent leur responsabilité civile si un particulier subit un préjudice à la suite d'une infraction. Le ministère de la Justice s'est donné pour mission de se concentrer sur un travail de prise de conscience afin que les entreprises et les administrations puissent développer des systèmes capables de protéger les informations capitales qui leur sont confiées par leur clientèle et par les usagers.

Protéger les enfants sur le Net

En tant que premier responsable du système judiciaire de l'État de Washington, j'ai la possibilité exceptionnelle de travailler avec les services de police, les procureurs, les législateurs et les groupes d'intérêt pour améliorer la sécurité publique. Dans le cadre de la campagne menée par nos services en faveur de la sécurité sur Internet (*SafetyNet)*, nos équipes se sont rendues sur le terrain dans l'État de Washington afin de faire partager ce que nous avons appris des experts sur les dangers d'Internet et pour parler des manières dont les enfants peuvent éviter ces dangers. Nous avons visité des écoles, rencontré les services de police et parlé avec des associations de parents d'élèves pour diffuser le message sur la sécurité.

En 2006, le ministère de la Justice s'est associé au Centre national pour les enfants disparus et exploités (*National Center for Missing & Exploited Children*), afin de proposer des séminaires de formation pour préparer 400 éducateurs et officiers de police à enseigner la sécurité sur Internet en utilisant un programme créé par une organisation appelée *NetSmartz*. En 2006, je me suis associé au *National Center for Missing & Exploited Children* avec des leaders de l'ensemble de l'État pour encourager 10 000 parents et responsables de mineurs à s'informer sur les questions de sécurité sur Internet et sur les procédés de prévention à travers *The Connected Family Online Classroom*, développée par la compagnie de télécommunications *Qwest*.

(25) RCW 19.255.010 and RCW 42.56.590, www.leg.wa.gov
(26) RCW 19.215.010, www.leg.wa.gov

© Cahiers de la sécurité -INHESJ

En 2007, j'ai formé l'Équipe Spéciale (*Task Force*) pour la sécurité des jeunes sur Internet, afin de renforcer la sensibilisation à la sécurité sur le Net dans l'État de Washington. Cette large coalition englobe les forces de police, les groupes d'intérêts de défense de l'enfant, les experts universitaires, les représentants du gouvernement à l'échelon local et de l'État, les entreprises de technologie et les associations, ainsi que les citoyens concernés. Les membres sont divisés en trois sous-comités, chacun se concentrant sur un problème particulier lié à la sécurité des jeunes sur Internet. Cette équipe spéciale révise, entre autres activités, la législation en cours dans des domaines apparentés tels que la pornographie impliquant des enfants et les communications illégales avec des mineurs.

En janvier 2008, les ministres de la Justice de tout le pays ont signé un accord avec *MySpace*, créant une équipe spéciale [27] afin de développer une technologie permettant de vérifier l'âge et l'identité des utilisateurs des sites de réseaux sociaux. *MySpace* et les ministres de la Justice se sont entendus sur une déclaration commune de principes fondamentaux dans laquelle nous mettons l'accent sur notre objectif commun de protéger les enfants des dangers de sites à teneur inappropriée et de contacts indésirables de la part d'adultes. Grâce à cet accord, *MySpace* a réalisé de gros progrès en matière de sécurité, comprenant le passage en revue d'images et vidéos afin d'y repérer un éventuel contenu nocif, et d'autres dispositions techniques destinées à protéger de nouveaux utilisateurs de moins de 18 ans contre tout contact en ligne indésirable avec un adulte. L'entreprise *MySpace* élimine aussi les profils électroniques créés par des délinquants sexuels fichés par la police.

MySpace travaille à établir les profils des utilisateurs de 16 et 17 ans en les gardant confidentiels, et prévoit de mettre en place un « verrouillage de l'âge », par lequel les utilisateurs qui indiquent qu'ils ont moins de 18 ans ne pourront pas modifier l'âge déclaré. L'accord exige aussi que la société dresse un registre des adresses électroniques fournies par les parents qui désirent restreindre l'accès de leur enfant au site. La société a créé des matériaux pédagogiques pour les parents, établi un service en ligne 24 heures sur 24 pour répondre aux enquêtes de la police, et formé plus de 3 500 policiers.

Nous sommes parvenus à un accord similaire avec *Facebook* en mai dernier et cette société a, elle aussi, rejoint l'équipe spéciale. Ce dernier rendra des comptes aux ministères de la Justice tous les trois mois et publiera un rapport officiel avec des conclusions et recommandations fin 2008.

Les défis qui demeurent

En dépit d'immenses progrès réalisés dans la surveillance du cyberespace, les entités publiques et privées demeurent confrontées à des défis. Dans un rapport adressé au Congrès en juin 2007, le *U.S. Government Accountability Office* décrivait plusieurs obstacles à la mise en œuvre de mesures contre le cybercrime, comme le manque de comptes-rendus précis des délits aux services de police ; la difficulté à obtenir et garder des enquêteurs, des procureurs et des experts en analyses d'ordinateurs ; les difficultés à rester au fait des technologies en cours et des techniques criminelles ; et le fait de travailler dans un environnement sans frontières.

À la différence des délits traditionnels, ceux qui sont perpétrés par le biais des réseaux informatiques peuvent être commis de loin, effectués automatiquement et sont en mesure d'attaquer un très grand nombre de victimes simultanément. Les auteurs peuvent rester plus facilement anonymes. Les enquêtes sont plus compliquées en raison de la nécessité de traiter avec de multiples juridictions, chacune ayant sa propre législation et ses procédures légales.

En dépit d'initiatives fréquentes et significatives destinées à informer les particuliers de leurs droits et des aides dont ils peuvent bénéficier, des études [28] laissent penser que 17 % d'Américains n'ont toujours pas de logiciels antivirus installés sur leur ordinateur et qu'environ un tiers n'utilise pas de logiciel pour bloquer ou enlever un spyware. Les chercheurs ont aussi découvert que la moitié des Américains possédant des connexions internet sans fil à domicile n'ont pas pris les précautions de base, telles que l'encodage. On estime à environ 3,7 millions le nombre de foyers américains possédant des raccordements avec des transmissions à large bande, et qui ne possèdent toujours pas de mur pare-feu.

Certaines études suggèrent que, sauf s'ils sont confrontés à un gros problème, les Américains ont tendance à ne pas se soucier de leurs informations personnelles, ni à prendre des dispositions pour limiter leur quantité susceptible d'être trouvée en ligne [29].

(27) L'équipe spéciale est dirigée par le Berkman Center for Internet and Society at Harvard University, http://cyber.law.harvard.edu/

(28) *Consumers Reports*, 2007, State of the Net report, www.consumerreports.org and McAfee-National Cyber Safety Alliance Online Safety Study, octobre 2007, www.staysafeonline.org

(29) «Privacy Implications of Fast, Mobile Internet Access», Pew Internet and American Life Project, février 2008, www.pewinternet.org

© Cahiers de la sécurité -INHESJ

L'importance des partenariats

Les partenariats constituent un élément clef pour combattre le cybercrime avec succès. Très tôt, les changements rapides dans la nature de la criminalité et de la technologie ont entraîné des partenariats presque involontaires entre citoyens, entreprises, gouvernement et police, alors que tous se débattaient pour trouver des moyens efficaces pour faire face à ces nouvelles menaces. Par exemple, dans le passé, un service chargé de faire respecter la loi et s'occupant d'instruire un procès n'aurait pu compter que sur la coopération amicale de fournisseurs de services internet acceptant de divulguer les informations nécessaires pour engager des poursuites judiciaires dans une affaire de cybercrime. Même la police disposant de ressources suffisantes pour ouvrir la voie sur ce nouveau front de la lutte anticriminelle trouvait qu'il était difficile de maîtriser le vaste univers en perpétuelle évolution de la criminalité sur Internet.

Heureusement, nous sommes aujourd'hui bien mieux armés pour lutter contre la délinquance high-tech. Il existe maintenant des mécanismes permettant d'assurer la coordination entre la police, les fournisseurs de services et d'autres. Par exemple, nos services ont travaillé en coopération avec Microsoft et AOL afin de rassembler l'information nécessaire pour engager des poursuites judiciaires contre des pourvoyeurs de spywares et de spams.

De plus, alors que les citoyens recherchent une plus grande protection contre la délinquance en ligne, le rôle du gouvernement évolue pour faire face à ces questions. L'Association nationale des ministres de la Justice (*National Association of Attorneys General*) anime une conférence annuelle sur le cybercrime pour fournir une formation en matière d'enquêtes, de législation, de procès et de campagnes d'éducation publique. Grâce à un effort de coopération, mis en place en 2003, entre notre association, le Centre national de la justice et l'État de droit de l'université du Mississippi (*National Center for Justice and The Rule of Law*), plus de 415 procureurs rattachés à des ministères de la Justice ont suivi une formation spéciale sur la criminalité électronique. J'ai personnellement dirigé deux séminaires sur la technologie pour des ministres de la justice et leurs équipes lors de nos réunions nationales.

Afin de réduire le nombre de victimes de ces comportements criminels, il est également crucial de renforcer la sensibilisation du public à l'importance de la protection des informations. Le ministère de la Justice de l'État de Washington s'est associé avec l'*American Association of Retired People* (AARP), Microsoft et la Commission fédérale du commerce, en 2006, pour présenter une Campagne de Cyber-sécurité, afin d'éduquer le public sur les dangers du Net, comme les faux courriers électroniques ou pages web, les virus et les spyware. La sécurité sur Internet fait aussi partie de notre programme d'éducation à la prévention contre le vol d'identité.

Les services de police s'équipent de nouvelles armes pour mener des enquêtes high-tech, car les traces et preuves d'actes criminels sont de plus en plus stockées sur des ordinateurs, des téléphones portables, des caméras numériques, dans des courriers électroniques, des messages et imageries électroniques. Les entreprises intensifient la sécurisation des données. Plus important encore, tous les acteurs reconnaissent maintenant que les partenariats ne sont pas seulement utiles, mais nécessaires et cruciaux afin de combattre et prévenir ce type de criminalité.

Conclusion

Le combat contre le cybercrime implique notre participation à tous – gouvernement, secteur privé, ainsi que le public. Le ministère de la Justice de l'État de Washington travaille intensément pour fournir un *leadership* à l'échelon de l'État, soutenir les services de police, éduquer les consommateurs, aider les entreprises et protéger les enfants. Les partenariats constituent la clef pour une réussite à long terme.

Rob McKENNA

© Cahiers de la sécurité -INHESJ

DOSSIER

Cybercriminalité : la recherche de profits

Myriam QUÉMÉNER

© Corbis

La délinquance économico-financière sur Internet prend désormais une importance croissante et constitue un fléau auquel les États doivent faire face de façon pertinente. La motivation principale des pirates est la recherche de profits, et la cybercriminalité, délinquance transnationale par excellence, est devenue une activité délictueuse des plus lucratives, qui permet de blanchir plus facilement l'argent issu de la criminalité classique. Il s'agit de cerner cette population de cyberdélinquants et leurs divers modes opératoires.

Cybercrime: The Profit Motive

The financial and economic delinquency of the internet have taken on a growing importance that has become a scourge that governments must deal with as effectively as possible. The principal motivation of hackers and cybercrime has become profit – the ultimate transnational delinquency which has become one of the most lucrative types of scams. It allows the easy laundering of money made by traditional criminal activities. It has become essential to better understand the various modes of operation of this kind of crime.

Myriam Quéméner

Magistrat depuis 1986, substitut général au service criminel de la Cour d'Appel de Versailles après avoir été précédemment sous-directrice à la direction des Affaires criminelles et des Grâces. Elle participe comme expert à des séminaires internationaux organisés par les ministères et le Conseil de l'Europe sur la cybercriminalité. Elle a écrit plusieurs articles sur la cybercriminalité et publié avec Joël Ferry, en 2007, *Cybercriminalité, défi mondial et réponses* aux éditions Economica.

© Cahiers de la sécurité -INHESJ

La cybercriminalité n'a rien de virtuel et tend aujourd'hui vers le crime organisé en parvenant à manipuler des sommes d'argent colossales. L'objectif des actions malveillantes est essentiellement lucratif, et la cybercriminalité est, désormais, structurée et essentiellement guidée par la recherche de profits importants en prenant peu de risques. Une enquête auprès de 2000 sociétés a révélé que la cybercriminalité coûte, en moyenne, 24 000 dollars par an à une entreprise américaine, soit 67 milliards de dollars à l'échelle des États-Unis. Le coût de la fraude, 2,7 millions d'euros en moyenne, reste élevé et, dans 41 % des cas, il s'accompagne d'autres dommages comme l'atteinte à l'image de l'entreprise.

Organisation des cyberdélinquants

La cybercriminalité est devenue l'affaire de professionnels et non plus le fait d'agissements d'étudiants en informatique ou d'amateurs. La recherche d'argent est le moteur essentiel de ces individus dont les activités sont désormais bien délimitées.

Les « hackers » ou pirates informatiques représentent l'ensemble des cybercriminels et sont, comme au niveau de la criminalité organisée, répartis en catégories spécialisées. Depuis quelques années, les hackers ont même leur rendez-vous européen [1], à savoir une conférence de haut niveau où se réunissent les meilleurs d'entre eux pour s'informer et échanger sur les techniques les plus innovantes.

Le « cracker » ou « chapeau noir », souvent confondu avec le hacker, pénètre les systèmes informatiques avec l'intention de nuire, et, en général, il essaye de tirer profit de ses méfaits, par exemple, porter préjudice à un concurrent, en acquérant des données confidentielles. Ils fonctionnent généralement comme des réseaux mafieux, pour leur propre compte ou le compte d'autrui. Souvent très performants techniquement, ils peuvent égaler les compétences des hackers et leur but est de maximiser cette connaissance à leur profit.

Certains jeunes commencent leur carrière dès l'adolescence. Dénommés « script kiddles », ils manipulent les ordinateurs sans mesurer les conséquences de leurs actes et constituent la main-d'œuvre de base. Âgés de 15 à 20 ans, les « kids » circulent sur les forums, achètent des listes de spams qu'ils revendent ensuite, et parviennent à se faire un peu d'argent en négociant des éléments utilisés pour commettre des fraudes. On trouve, par exemple, ce type de jeunes en Ukraine. Ils sont la vraie « main-d'œuvre » en la matière. Ce trafic leur génère des revenus mensuels modestes et ils se font parfois « arnaquer » eux-mêmes.

Les « codeurs » ont une expérience supérieure à cinq ans dans le monde des hackers. Âgés de 20 à 25 ans, ils ont un rôle de programmeurs professionnels et sont parfois autodidactes. Ils vendent généralement des outils prêts à l'emploi comme des « bots » faits sur mesure, ou des chevaux de Troie.

Les « drops », sensiblement plus âgés que les kids, jouent un rôle incontournable dans la cybercriminalité et transforment l'argent « virtuel » en vrai argent. Ils offrent aux criminels l'opportunité de transférer l'argent volé sur leurs propres comptes en banque. Une fois l'opération effectuée, ils gardent un pourcentage, généralement de l'ordre de 50 % des montants transférés. La condition essentielle pour devenir un drop, mis à part le fait d'avoir un compte en banque, est de résider dans un pays ne réprimant pas les délits numériques comme, par exemple, l'Indonésie, la Malaisie et la Bolivie. Cette organisation démontre que les délinquants profitent des « cyberparadis » et pose le problème de la nécessité de créer une législation mondiale de lutte contre la cybercriminalité.

Une « mule » est une personne utilisée pour transporter des objets illicites telles des armes ou- de la drogue, et ce, parfois à son insu. Sur Internet, les mules sont recrutées par e-mail pour « transporter de l'argent » contre rémunération, l'objectif du fraudeur pouvant être le vol, le détournement d'argent, le blanchiment d'argent, etc. Pour la recruter, le pirate abuse un internaute qui se rend ainsi complice d'une fraude, de vol, de détournement ou de blanchiment d'argent passible de poursuites. Les cyberdélinquants envoient, par exemple, des e-mails proposant de devenir le collaborateur d'une prétendue société financière internationale. Parfois, un pseudo-contrat de travail est joint pour rendre l'offre plus crédible. Il est indiqué à l'internaute qu'il recevra des fonds sur son compte bancaire et qu'il devra les transférer vers un autre compte. En tant qu'intermédiaire, il percevra une commission pouvant aller jusqu'à 3 000 euros par mois via *Western Union*. Le cyber-escroc utilise donc un autre compte pour faire transiter cet argent d'origine frauduleuse et le transfère dans un autre pays. Les mules sont ainsi utilisées pour brouiller les pistes d'analyse d'une fraude et rendre beaucoup plus difficile, voire impossible la

(1) *Cf.* « black Hat Europe 2008, le rendez-vous européen des hackers », revue *Mag Securs*, avril-juin 2008.

© Cahiers de la sécurité -INHESJ

récupération des fonds. Le risque pour la personne servant de mule est d'être mise en examen pour complicité de fraude et poursuivie pénalement.

Certaines mafias ont également investi ce domaine, ce qui permet d'affirmer que la cybercriminalité est une délinquance commise en bande organisée. Cerner l'ampleur de l'implication des mafias n'est pas chose aisée, même si de fortes présomptions existent et des certitudes concernant l'action des mafias [2], par exemple en Roumanie, qui sont spécialisées dans le domaine du « carding ». Le piratage des systèmes bancaires est très souvent le fait d'organisations criminelles organisées, souvent d'Europe de l'Est.

En effet, de nombreux groupes criminels ont très vite compris que l'anonymat et la liberté que procure Internet permet assez facilement des opérations de blanchiment d'argent et, à cet égard, le domaine des jeux en ligne est un terrain très lucratif.

L'utilisation facile de « e-gold » en a fait un moyen de paiement universel. E-gold possède aussi trois caractéristiques essentielles pour les cybercriminels, à savoir l'anonymat car il est possible d'ouvrir un compte e-gold en moins d'une minute ; l'absence de vérification ; et enfin aucune obligation de donner une adresse e-mail valide. D'autres devises électroniques sont aussi largement utilisées dans les échanges entre criminels Web, mais e-gold est la référence en matière de transactions entre les cyberdélinquants. Il s'agit des transferts offerts par *Money Gram* ou encore *Western Union* qui sont irréversibles, quasiment anonymes et traversant les frontières presque instantanément puisque, même si, en théorie, une pièce d'identité est exigée pour recevoir l'argent liquide, en pratique, les bureaux dans certains pays ne font pas de vérifications.

Il existe des sites sur lesquels il est possible d'acheter des objets avec une carte volée, appelés sites « cartable ». Ces sites sont des magasins « on-line » qui n'exigent pas que l'adresse de facturation et de livraison soit la même. Ainsi, les criminels achètent des marchandises on-line, les font livrer aux drops qui les leur retournent, et, ensuite, la marchandise est vendue sur des sites aux enchères en ligne.

Voilà un scénario typique pour de l'extorsion en ligne : une compagnie qui fait de la vente sur Internet reçoit un e-mail menaçant. Elle doit payer 10 000 dollars sinon son site Internet serait estropié. La compagnie ignore le mail et, quelques jours après, son serveur bloque, ce qui entraîne des pertes d'argent considérables. Ensuite, arrive un deuxième mail, cette fois-ci demandant 40 000 dollars. En cas de non-paiement, la compagnie risque encore des pertes. En revanche, si elle paie, on lui offre généreusement une protection pendant un an. Après avoir fait le calcul, la compagnie paie.

La criminalité en ligne agit de façon plus mobile que jamais. Ainsi, le « phishing », qui semblait trouver sa source pour 60 % dans des organisations russes piratant des sites européens au cours du premier semestre 2007, s'est tourné vers la Chine pour installer ses activités en ligne au cours du second semestre. Les pays peu protégés ou mal équipés sont les premiers visés. Le Pérou fournit ainsi 9 % des attaques en ligne contre les vingt-cinq pays les mieux équipés en haut débit, alors que 80 % de ses internautes utilisent des cybercafés. Le marché de la piraterie informatique existe désormais. Par exemple, pour faire envoyer 20 millions d'e-mails indésirables, le tarif est de 314 euros et la location d'un serveur permettant d'envoyer 74 millions de spams chaque mois coûte 396 euros [3].

On assiste aujourd'hui à la banalisation des outils de piratage qui sont désormais accessibles à presque tous les pays. Ce commerce est considéré comme plus rentable que celui du trafic des stupéfiants et souvent moins risqué. Des sites vendent d'ailleurs des kits de piratage pour la somme de 10 dollars et de phishing pour 5 dollars par exemple [4]. Ils facilitent la mise en ligne de sites Internet frauduleux, calqués sur des sites véritables tout en gérant l'envoi massif de courriels incitant les internautes à se connecter aux fausses pages afin de récupérer le plus de données. Les experts en cybercriminalité de l'*Internet Security System* d'IBM [5] ont ainsi découvert qu'il était possible de louer les services d'un réseau d'ordinateurs infectés par un programme malveillant dénommé Botnet, constitué de 150 000 PC, pour la somme de 350 $ par semaine. Il apparaît que les tarifs dépendent souvent de la taille de ce réseau et il faut compter un minimum de 100 euros pour quelques heures. Ainsi, des cybercriminels

(2) *Cf.* Guillaume Lovet, « L'argent sale sur le net : les modèles économiques des cybercriminels », *Revue de la Défense Nationale et Sécurité Collective*, mai 2008.

(3) *Cf.* Gerric Poncet, « les tarifs de la cybercriminalité », en date du 2 juillet 2008, site : www.lepoint.fr

(4) Voir la revue Mag Securs, n° 18, p. 33, interview de Guillaume Lovet.

(5) *Cf.* le blog de la *X-Force Intelligence*.

© Cahiers de la sécurité -INHESJ

peuvent le louer pour mener une opération de spams. Leur but est de saturer les serveurs de messagerie des grandes entreprises sous l'importance du trafic. Par exemple, pour un tarif variant de 2 à 25 $, le pirate peut fournir des informations de carte de crédit, le prix étant fonction des informations disponibles tels le code, la date d'expiration, le nom du propriétaire...).

Actuellement, des boîtes à outils informatiques vendues sur le marché noir de la criminalité diffusent deux nouvelles tendances, à savoir la modification furtive des navigateurs et la transformation discrète des pages Internet par phishing. D'autres moyens de piratage circulent sur la Toile et permettent de constater que tout se vend sur Internet comme les numéros de carte de crédit facturés environ entre 0,5 et 5 dollars pièce ou les coordonnées bancaires entre 30 et 400 dollars.

Depuis deux ans environ, une véritable économie souterraine consistant à faire commerce des failles de sécurité et de kits de « malwares » (logiciels malveillants) s'est développée en raison de son caractère lucratif. Il existe même des bourses aux échanges, véritable marché noir où non seulement les failles de sécurité, mais également les informations collectées, tels les numéros de sécurité sociale ou de passeport, les adresses électroniques et physiques peuvent se monnayer au cours du jour. Il s'agit d'activités qui démontrent à l'évidence la créativité des cyberdélinquants qui adaptent sans cesse leurs modes opératoires, qui se diversifient et évoluent constamment.

Typologies des cyberfraudes

Le « carding » est le piratage de cartes bancaires par diverses techniques matérielles, logicielles ou subversives aux fins d'obtenir et de revendre les données de cartes bancaires, de s'en servir pour effectuer des achats frauduleux, au préjudice du porteur légal. Le carding se décline en trois étapes, à savoir le « coding », qui n'est autre que le piratage des données, le « vending » ou revente des numéros de cartes bancaires et des informations sur le titulaire, enfin, le « cashing » qui regroupe les échanges financiers délictueux comme les escroqueries et le blanchiment d'argent. Une fois ces informations récupérées, il s'agit de les monnayer discrètement. Pour ce faire, de nombreuses sociétés de ventes commerciales virtuelles voient le jour afin de générer de faux achats mais de véritables transactions.

Le « skimming » est une criminalité essentiellement d'Europe de l'Est, en particulier de Bulgarie et de Roumanie. Il s'agit du piratage de distributeur automatique de billets (DAB), à l'aide notamment de faux claviers et de micros-caméras. Le nombre de ces attaques ne cesse de croître ; ainsi 520 distributeurs ont été piratés en 2006, contre 200 en 2005 et 80 en 2004. À l'heure actuelle, les banques réagissent, et ce type d'affaire devrait progressivement diminuer.

Le « spamming » [6] désigne l'envoi massif et automatique de messages électroniques non sollicités, généralement adressés à des fins publicitaires, voire frauduleuses. À l'heure actuelle, leur part est évaluée à plus de 80 % du trafic e-mail total [7] et 16 milliards de spams seraient envoyés chaque jour en Europe. Les spams peuvent être de simples publicités, mais aussi des messages émis par des virus et les propageant, des incitations à visiter des sites frauduleux qui capturent des informations confidentielles.

Des formes dérivées de spamming se sont développées ces dernières années, surnommées « arnaque à la nigériane » ou fraude 4-1-9 [8], qui ont pour objectif d'abuser de la crédulité des internautes en utilisant les messageries électroniques pour leur soutirer de l'argent. Cette tromperie repose sur un envoi de mails visant à faire croire à la victime que l'expéditeur possède une importante somme d'argent comme des fonds à placer à l'étranger suite à un changement de contexte politique et fait part de son besoin d'utiliser un compte existant pour transférer cet argent. Pour crédibiliser le scénario, les fraudeurs mettent en place de faux sites bancaires qui usurpent l'identité d'établissements internationaux. Ces derniers visent à faire croire aux victimes que l'argent promis existe réellement.

Les réseaux sociaux constituent le nouveau moyen de diffusion des « scams » nigérians « 419 ». Ce phénomène a été observé pour la première fois par les chercheurs des laboratoires *BitDefender* sur le site Internet de réseaux professionnels *LinkedIn*, mais d'autres sites de réseau sociaux peuvent également en être la cible. L'email de scam est envoyé sous la forme d'une invitation qui est un

(6) Ou « pourriel », terme choisi en référence à un célèbre sketch des Monty Python, troupe comique britannique, parodiant une publicité radiophonique pour le Spam, une sorte de jambon épicé, pendant laquelle la marque Spam était répétée à de multiples reprises.

(7) Source : direction du Développement des médias.

(8) Fraude dénommée 4-1-9 en référence à l'article du Code pénal nigérian interdisant cette pratique.

© Cahiers de la sécurité -INHESJ

moyen par lequel un utilisateur demande à être ajouté au réseau social d'un autre utilisateur. Cette requête est appuyée par une page de profil construite qui semble authentifier la demande de mise en relation du fraudeur. Ces messages ne pouvant être envoyés que par les titulaires de comptes du réseau social en contournant complètement les filtres antispams.

Cette nouvelle forme du procédé de scam 419 est plus dangereuse que les précédentes, car les probabilités de se faire piéger pour les utilisateurs du réseau sont beaucoup plus importantes puisqu'ils utilisent cet outil pour développer leurs affaires ou leur carrière, et ont donc tendance à lui accorder une confiance implicite. Le réseau social ne vérifie en aucune façon l'identité des personnes s'inscrivant sur le site, ce qui peut parfois donner lieu à des dérapages comme, par exemple, lors d'un incident récent où des sites pornographiques ont ajouté des pages utilisateurs « sur mesure » sur le réseau social de manière à améliorer leur référencement sur les moteurs de recherche. L'envoi de spams nombreux peut donner lieu à des poursuites sur la base de la loi Godfrain.

Le phishing [9] et le « pharming » [10] sont deux techniques permettant de faire croire aux victimes qu'elles se trouvent sur un site Web sécurisé, leur banque par exemple, alors qu'elles sont en fait sur un site Web factice où leurs informations bancaires vont leur être dérobées. La première utilise le spam pour attirer leur victime sur un faux site. La seconde consiste à rediriger les victimes vers le faux site Web alors qu'elles ont bien tapé une adresse Web correcte dans leur navigateur.

Si les banques anglo-saxonnes ont été les premières cibles des cyber-escrocs, désormais tous les établissements bancaires européens sont visés, et 90 % des attaques par phishing concernent des établissements financiers. Ces cyber-escrocs peuvent récupérer jusqu'à 400 fois la mise initiale [11]. Plus ou moins discrète en ciblant l'humain, elle est actuellement en forte progression, mais pour le moment très peu d'informations concrètes, de cas d'attaques sont disponibles, car les entreprises sont particulièrement réservées sur ce sujet, n'osant évoquer qu'elles puissent en avoir été victimes. C'est une technique de fraude qui vise aussi bien les particuliers que les entreprises et le secteur bancaire. Les forums de phishing représentent un marché pour les acheteurs et vendeurs d'informations financières volées. Les acheteurs peuvent être aussi bien des individus que des organisations criminelles.

Pour 100 000 mails, envoyés, les pirates récoltent environ vingt comptes bancaires à soldes différents. Par la suite, ils peuvent, soit vendre l'information pour une valeur entre 100 $ et 500 $ par compte, payable par e-gold, soit transformer l'argent virtuel en vrai argent via les drops. Évidemment, la deuxième solution rapporte plus, mais elle comporte plus de risques aussi - il s'agit de trouver un drop à qui on fait confiance.

Ce sont des manifestations de la criminalité organisée, et ces techniques, qui peuvent être qualifiées juridiquement d'escroqueries en bande organisée [12], sont souvent traitées par les juridictions interrégionales spécialisées (JIRS). Elles peuvent également être sanctionnées sur le fondement de l'infraction de collecte frauduleuse de données nominatives en application de l'article 226-18 du code pénal [13]. Car, au final, le pirate se procure des données personnelles et les traite de manière frauduleuse informatiquement.

Des escrocs utilisent également le téléphone portable pour tenter de récupérer les identifiants bancaires de leurs victimes. Par exemple, un SMS envoyé sur le téléphone mobile des victimes confirme leur inscription à un site payant de rencontre sur Internet alors qu'elles n'ont rien demandé. Pour ne pas payer, le SMS leur demande d'annuler l'inscription en se connectant à un site Internet qui est, en fait, un site pirate qui va installer un cheval de Troie à leur insu et voler des informations personnelles, comme les identifiants bancaires.

Désormais, on assiste aussi à l'exploitation des réseaux sociaux comme *Facebook* ou *Linked-In* par des cyber-criminels. Ces réseaux, qui concentrent une quantité phénoménale d'informations personnelles, permettent de rassembler suffisamment d'éléments pour se substituer à l'identité des utilisateurs. Le détournement de l'identité d'un individu, la récupération d'éléments à caractère personnel vont ensuite leur servir pour se faire passer pour un autre afin de commettre des délits, des achats avec des moyens de paiement usurpés.

DOSSIER

(9) Contraction des mots anglais *phreaking,* fraude informatique et *fishing* (pêche) se traduisant parfois en « hameçonnage, filoutage ».

(10) Le terme pharming provient de la contraction des mots anglais *farming* et *phone phreaking,* qui pourrait se traduire par « piratage de lignes téléphoniques ».

(11) *Cf.* Guillaume Lovet, *op. cit.*

(12) Article 312-2 du Code pénal.

(13) Cette infraction est punie de cinq ans d'emprisonnement, et de 300 000 euros d'amende.

© Cahiers de la sécurité -INHESJ

Ce « business parallèle » est difficilement mesurable, mais il ne cesse de se développer depuis plusieurs années, ce qui démontre l'existence d'un « marché ». Ce type d'arnaque joue sur la curiosité, la naïveté ou l'appât du gain des internautes. Le client est informé qu'il ne faut jamais laisser ses coordonnées sur le réseau. Il est le principal artisan de sa sécurité. Par ailleurs, les procédés évoluent et sont de plus en plus rusés, des cyberdélinquants font, en effet, du prosélytisme en matière de sécurité. Ainsi, de récents courriels frauduleux, très convaincants, mettent en garde les clients de banques contre le filoutage, rappelant que les banques ne demanderont jamais de détails sur un compte par courriel, et les invitant à signaler tout message suspect. Mis en confiance par ces avertissements, le client va être tenté de cliquer pour signaler le site et c'est alors que la victime va être redirigée vers un site frauduleux.

En conclusion, on comprend aisément que la lutte contre la cybercriminalité implique une mobilisation sans faille de l'ensemble des acteurs et un renforcement de la coopération internationale. Les données circulent à la vitesse de la lumière et sont difficiles à pister. La cybercriminalité pose de nombreux défis et dans le « cybermonde » qui évolue sans cesse, les services de police et de justice luttant contre la cybercriminalité doivent mettre en place des stratégies d'anticipation des menaces et de répression au risque de mettre en péril les internautes et de freiner le développement de la société du numérique.

Myriam QUÉMÉNER

© Cahiers de la sécurité -INHESJ